多输出布尔函数与布尔函数代数免疫阶之间的关系

王秋艳,金晨辉
(信息工程大学电子技术学院,河南郑州 450004)

摘 要: 本文给出了多输出布尔函数状态函数集合的代数结构,证明了多输出布尔函数的代数免疫阶等于某布尔函数的代数免疫阶,且该布尔函数是多输出函数的分量函数的一个非零非线性组合.接着证明了该组合的代数免疫阶是所有非零非线性组合中最小的,从而得出多输出布尔函数的代数免疫阶等于其所有非零非线性组合代数免疫阶的最小值.

关键词: 代数攻击;多输出布尔函数;代数免疫阶;状态函数
中图分类号: TN918.1 **文献标识码:** A **文章编号:** 0372-2112 (2011) 01-0124-04

Relationship Between the Algebraic Immunity of Multi-Output Boolean Functions and Boolean Functions

WANG Qiu-yan, JIN Chen-hui
(*Electronic Technology Institute, Information Engineering University, Zhengzhou, Henan* 450004, *China*)

Abstract: This paper presents the algebraic structure of the conditional equations set for multi-output Boolean functions, proves that the algebraic immunity of multi-output Boolean functions is equal to that of a certain Boolean function, which is a combination of the component functions for multi-output Boolean functions, and among all combinations, this one has the minimum algebraic immunity. Hence, it can be concluded that the algebraic immunity of multi-output Boolean functions is equal to the minimum of algebraic immunities of all combinations.

Key words: algebraic attack; multi-output Boolean functions; algebraic immunity; conditional equations

1 引言

近年来,代数攻击作为一种新的密码体制的攻击方法受到人们的广泛关注,人们对它的研究也做了大量的工作[1~3].它的基本思想是将密码系统用一个大的多变元方程组来表示,通过求解该方程组可以恢复出密钥.代数攻击对于基于线性反馈移位寄存器的序列密码构成威胁.序列密码中所使用的布尔函数应具有高的代数次数,但如果高次数的布尔函数具有低次零化子,攻击者可利用该零化子得到关于密钥的低次方程组,求解该方程组从而恢复密钥[4].代数攻击的提出对密码系统中所使用的布尔函数提出了更高的要求,为了衡量布尔函数抵抗代数攻击的能力,Meier 等[4]提出了布尔函数的一个新的密码学性质——代数免疫性,使用具有高的代数免疫阶的布尔函数是抵抗代数攻击的必要条件.近年来,对布尔函数的代数免疫阶已进行了比较深入的研究,在计算零化子和代数免疫阶的快速算法、代数免疫阶最优的布尔函数的构造等方面取得了许多重要成果[4~7].

在密码设计中,很多情况下需要考虑多输出布尔函数的情况,如序列密码的前馈函数、分组密码的 S 盒设计中就经常用到多输出布尔函数.2007 年,Fischer 和 Meier 在文献[8]中对多输出布尔函数提出了一种代数分析方法,攻击者可利用多输出布尔函数的状态函数得到关于密钥的低次方程组,并定义了多输出布尔函数代数免疫阶的概念.但由于多输出布尔函数讨论起来比较复杂,目前公开文献中关于多输出布尔函数的状态函数和代数免疫阶的比较深入的研究尚不多见.

本文给出了多输出布尔函数的状态函数集合的代数结构,证明了多输出布尔函数的代数免疫阶等于某布尔函数的代数免疫阶,且该布尔函数是代数免疫阶最小的分量函数的非零非线性组合,从而证明了多输出布尔函数的代数免疫阶等于其分量的所有非零非线性组合的代数免疫阶的最小值,把多输出布尔函数的代数免疫问题转化为布尔函数的代数免疫问题,为研究多输出布尔函数的代数免疫阶的相关问题奠定了理论基础.

收稿日期:2009-12-09;修回日期:2010-05-11

2 基本概念

在本文中,用"⊕"表示有限域 F_2 中的加法. n 元布尔函数 $f(x)$是从 F_2^n 到 F_2 的一个映射,多输出布尔函数 $F(x)$是从 F_2^n 到 F_2^m 的一个映射,记为 $F(x):F_2^n\to F_2^m$,它可以表示为 $F(x)=(f_1(x),\cdots,f_m(x))$,其中每个分量函数 $f_i(x)$为 n 元布尔函数,$i=1,2,\cdots,m$.

定义 1[4]　设 $f(x)$为 n 元布尔函数,则称 $f(x)$和 $f(x)\oplus 1$ 的所有零化子的代数次数最小值为 $f(x)$的代数免疫阶,记为 $AI(f)$.并记 $f(x)$的所有零化子和零函数的集合为 $An(f)$,记 $f(x)$的所有零化子的代数次数最小值为 $\min\deg(An(f))$.

定义 2[8]　设 $F(x):F_2^n\to F_2^m$ 是多输出布尔函数,给定输出 $y\in F_2^m$,若存在 n 元布尔函数 $F_y(x)$使得任意 $x\in F^{-1}(y)$都有 $F_y(x)=0$,则称 $F_y(x)$为输出 y 的状态函数.记 $AI_y(F)$为输出 y 的非零状态函数的代数次数的最小值,当输出 y 遍历时称 $AI_y(F)$的最小值为多输出函数 $F(x)$的代数免疫阶,记为 $AI(F)$.

以下记 $An_y(F)$为多输出函数 $F(x)$在输出 y 的所有状态函数构成的集合.

3 关于多输出布尔函数的代数免疫阶的几点结论

Meier 等在文献[4]中给出了下述结论.

引理 1[4]　设 $f(x)$为 n 元布尔函数,则 $f(x)$的所有零化子和零函数的集合是由 $1\oplus f$ 在 n 元布尔函数集上生成的理想,即 $An(f)=\{(1\oplus f)g:g$ 是 n 元布尔函数$\}=<1\oplus f>$.

下面我们给出了刻画多输出布尔函数状态函数集合的代数结构的定理,首先给出一个引理.

引理 2　设 $f_1(x),f_2(x),\cdots,f_m(x)$为 n 元布尔函数,$m\geqslant 2$,则有

$$<f_1,f_2,\cdots,f_m>=<1\oplus\prod_{i=1}^{m}(f_i\oplus 1)>$$

证明　由于 $1\oplus\prod_{i=1}^{m}(f_i\oplus 1)=\bigoplus_{\substack{1\leqslant k_1\leqslant\cdots\leqslant k_s\leqslant m\\ 1\leqslant s\leqslant m}} f_{k_1}\cdots f_{k_s}\in <f_1,f_2,\cdots,f_m>$,故 $<1\oplus\prod_{i=1}^{m}(f_i\oplus 1)>\subseteq<f_1,f_2,\cdots,f_m>$.

下面证明 $<f_1,f_2,\cdots,f_m>\subseteq<1\oplus\prod_{i=1}^{m}(f_i\oplus 1)>$.

对任意 $h\in<f_1,f_2,\cdots,f_m>$,有 $h=\bigoplus_{j=1}^{m}f_jg_j$,其中 g_j 为 n 元布尔函数,则

$$h\prod_{i=1}^{m}(f_i\oplus 1)=\bigoplus_{j=1}^{m}f_jg_j\prod_{i=1}^{m}(f_i\oplus 1)=\bigoplus_{j=1}^{m}(f_jg_j\prod_{i=1}^{m}(f_i\oplus 1))$$

$$=\bigoplus_{j=1}^{m}(f_jg_j\cdot(f_j\oplus 1)(f_1\oplus 1)\cdots(f_{j-1}\oplus 1)(f_{j+1}\oplus 1)\cdots(f_i\oplus 1))=0,$$

故 h 是 $\prod_{i=1}^{m}(f_i\oplus 1)$的零化子,即 $h\in An(\prod_{i=1}^{m}(f_i\oplus 1))$.

由引理 1 可知,$An(\prod_{i=1}^{m}(f_i\oplus 1))=<1\oplus\prod_{i=1}^{m}(f_i\oplus 1)>$,故 $h\in<1\oplus\prod_{i=1}^{m}(f_i\oplus 1)>$.因而 $<f_1,f_2,\cdots,f_m>\subseteq<1\oplus\prod_{i=1}^{m}(f_i\oplus 1)>$.

综上,$<f_1,f_2,\cdots,f_m>=<1\oplus\prod_{i=1}^{m}(f_i\oplus 1)>$.

证毕.

定理 1　设 $F(x):F_2^n\to F_2^m$ 为多输出布尔函数,$F(x)=(f_1(x),\cdots,f_m(x))$,$y=(y_1,y_2,\cdots,y_m)\in F_2^m$,则状态函数集合 $An_y(F)$是由 $f_1\oplus y_1,f_2\oplus y_2,\cdots,f_m\oplus y_m$ 在 n 元布尔函数集上生成的理想,即 $An_y(F)=<f_1\oplus y_1,f_2\oplus y_2,\cdots,f_m\oplus y_m>$.

证明　先证 $<f_1\oplus y_1,f_2\oplus y_2,\cdots,f_m\oplus y_m>\subseteq An_y(F)$.

设 $g(x)\in<f_1\oplus y_1,f_2\oplus y_2,\cdots,f_m\oplus y_m>$,则 $g(x)=\bigoplus_{i=1}^{m}g_i(f_i\oplus y_i)$,其中 g_i 为 n 元布尔函数.由于对任意的 $x\in F^{-1}(y)$均有 $f_i=y_i$,故 $g(x)=0$,即 $g(x)\in An_y(F)$.因而 $<f_1\oplus y_1,f_2\oplus y_2,\cdots,f_m\oplus y_m>\subseteq An_y(F)$.

下面证明 $An_y(F)\subseteq<f_1\oplus y_1,f_2\oplus y_2,\cdots,f_m\oplus y_m>$.

对任意 $g(x)\in An_y(F)$,令 $h=\prod_{i=1}^{m}(f_i\oplus y_i\oplus 1)$,则 $h(x)=1$ 当且仅当 $F(x)=y$,即 $F^{-1}(y)=\{x\in F_2^n:h(x)=1\}$,故由定义 $g(x)$是 $h(x)$的零化子,则由引理 1 可得 $g\in<h\oplus 1>$,从而 $An_y(F)\subseteq<h\oplus 1>$.又由引理 2 的证明可知 $h\oplus 1\in<f_1\oplus y_1,f_2\oplus y_2,\cdots,f_m\oplus y_m>$,故 $<h\oplus 1>\subseteq<f_1\oplus y_1,f_2\oplus y_2,\cdots,f_m\oplus y_m>$,从而 $An_y(F)\subseteq<f_1\oplus y_1,f_2\oplus y_2,\cdots,f_m\oplus y_m>$.

综上所述,$An_y(F)=<f_1\oplus y_1,f_2\oplus y_2,\cdots,f_m\oplus y_m>$.

证毕.

定理 2　设 $F(x):F_2^n\to F_2^m$ 为多输出布尔函数,$F(x)=(f_1(x),\cdots,f_m(x))$,$y=(y_1,y_2,\cdots,y_m)\in F_2^m$,则有:

(1)若布尔函数 $h_y(x)=\prod_{i=1}^{m}(f_i\oplus y_i\oplus 1)$,则 $AI_y(F)=\min\deg(An(h_y))$.

(2)特别的,设 $F(x)$在 $y^*\in F_2^m$ 处达到代数免疫阶,则 $AI(F)=AI(h_{y^*})$.

证明　(1)由引理 1 和定理 1 可知,$An(h_y)=<1\oplus h_y>=<1\oplus\prod_{i=1}^{m}(f_i\oplus y_i\oplus 1)>$,$An_y(F)=<f_1\oplus y_1,f_2$

$\oplus y_2,\cdots,f_m\oplus y_m>$,又由引理 2 可知 $<f_1\oplus y_1,f_2\oplus y_2,\cdots,f_m\oplus y_m>=<1\oplus\prod_{i=1}^{m}(f_i\oplus y\oplus 1)>$,即 $An_y(F)=An(h_y)$,从而由定义得 $AI_y(F)=\min\deg(An(h_y))$.

(2)若 $F(x)$在 $y^*\in F_2^m$ 处达到代数免疫阶,则由结论(1)可知 $AI(F)=AI_{y^*}(F)=\min\deg(An(h_{y^*}))$.又由于 $h_{y^*}(x)=\prod_{i=1}^{m}(f_i\oplus y_i{}^*\oplus 1)\in\langle f_1\oplus y_1{}^*\oplus 1,\cdots,f_m\oplus y_m{}^*\oplus 1\rangle$,故$\langle h_{y^*}(x)\rangle\subseteq\langle f_1\oplus y_1{}^*\oplus 1,\cdots,f_m\oplus y_m{}^*\oplus 1\rangle$,设 $z=(y_1{}^*\oplus 1,\cdots,y_m{}^*\oplus 1)$,从而 $An(h_{y^*}\oplus 1)\subseteq An_z(F)$,由定义可知 $\min\deg(An(h_{y^*}\oplus 1))\geqslant AI_z(F)\geqslant AI(F)=\min\deg(An(h_{y^*}))$,因而 $AI(h_{y^*})=\min\deg(An(h_{y^*}))$,从而有 $AI(F)=AI(h_{y^*})$.

证毕.

该定理给出了多输出布尔函数的一个重要性质.利用这个性质,可以将多输出函数的代数免疫问题转化为布尔函数的代数免疫问题.

引理 3 设 $g(x)$是 m 元布尔函数,且 $g(x)\neq 1$,$x=(x_1,x_2,\cdots,x_m)\in F_2^m$,则存在 $b=(b_1,b_2,\cdots,b_m)\in F_2^m$ 使得 $g(x)\in<x_1\oplus b_1,x_2\oplus b_2,\cdots,x_m\oplus b_m>$.

证明 设 $g(x)=a_0\bigoplus_{\substack{1\leqslant k_1\leqslant\cdots\leqslant k_s\leqslant m\\1\leqslant s\leqslant m}}\beta_i x_{k_1}x_{k_2}\cdots x_{k_s}$,其中 $\beta_i\in F_2,1\leqslant i\leqslant 2^m-1$.

若 $g(x)$不含常数项,即 $a_0=0$,则 $g(x)=\bigoplus_{\substack{1\leqslant k_1\leqslant\cdots\leqslant k_s\leqslant m\\1\leqslant s\leqslant m}}\beta_i x_{k_1}x_{k_2}\cdots x_{k_s}\in<x_1,x_2,\cdots,x_m>$.取$(b_1,b_2,\cdots,b_m)=0$,则显然有 $g(x)\in<x_1\oplus b_1,x_2\oplus b_2,\cdots,x_m\oplus b_m>$.

若 $g(x)$含常数项,即 $a_0=1$,已知 $g(x)\neq 1$,故存在 $c=(c_1,c_2,\cdots,c_m)\in F_2^m$,使得 $g(c)=0$.另 m 元布尔函数 $h(x)=g(x\oplus c)$,则 $h(0)=g(c)=0$,即 $h(x)$不含常数项,由前面证明可知 $h(x)\in<x_1,x_2,\cdots,x_m>$.又因为 $g(x)=g(x\oplus c\oplus c)=h(x\oplus c)\in<x_1\oplus c_1,x_2\oplus c_2,\cdots,x_m\oplus c_m>$,取 $b=c$,则 $g(x)\in<x_1\oplus b_1,x_2\oplus b_2,\cdots,x_m\oplus b_m>$.

证毕.

定理 3 设 $F(x):F_2^n\to F_2^m$ 为多输出布尔函数,$F(x)=(f_1(x),\cdots,f_m(x))$,且 $F(x)$在输出 y^* 达到代数免疫阶,$y^*=(y_1{}^*,y_2{}^*,\cdots,y_m{}^*)\in F_2{}^m$,布尔函数 $h_{y^*}(x)=\prod_{i=1}^{m}(f_i\oplus y_i{}^*\oplus 1)$,记 $AI_N(F)$为 $F(x)$分量函数所有非零非线性组合的代数免疫阶的最小值,则有 $AI(h_{y^*})=AI_N(F)$.

证明 设 $g(x)$为任意的非零 m 维布尔函数,则 $g\circ F(x)$为 $F(x)$分量函数的非零非线性组合,由引理 3 可知存在 $y=(y_1,y_2,\cdots,y_m)\in F_2^m$,使得布尔函数 $g\circ F(x)\oplus 1\in<f_1\oplus y_1,f_2\oplus y_2,\cdots,f_m\oplus y_m>$,故 $<g\circ F(x)\oplus 1>\subseteq<f_1\oplus y_1,f_2\oplus y_2,\cdots,f_m\oplus y_m>$,即 $An(g\circ F(x))\subseteq AI_y(F)$.当 $g(x)$取遍所有非零布尔函数时,$F(x)$的非零非线性组合的零化子集合总包含于某输出 y 的状态函数集合中,则由定义显然有 $AI_N(F)\geqslant AI(F)$.又因$F(x)$在 $y^*\in F_2^m$ 处达到代数免疫阶,由定理 2 可知$AI(F)=AI(h_{y^*})$,故 $AI_N(F)\geqslant AI(h_{y^*})$.且 h_{y^*}是 $F(x)$分量函数的一种非零非线性组合,则$AI_N(F)\leqslant AI(h_{y^*})$,因而 $AI(h_{y^*})=AI_N(F)$.

证毕.

推论 1 设 $F(x):F_2^n\to F_2^m$ 是多输出布尔函数,则 $AI_N(F)=AI(F)$.

证明 设 $F(x)$在 $y^*\in F_2^m$ 处达到代数免疫阶,则由定理 2 和定理 3 可知,$AI(F)=AI(h_{y^*})$,$AI(h_{y^*})=AI_N(F)$,故 $AI(h_{y^*})=AI_N(F)$.

证毕.

4 结束语

本文对多输出布尔函数的代数免疫阶进行了深入的分析和研究,给出了多输出函数的状态函数集合的代数结构,证明了多输出布尔函数的代数免疫阶等于某布尔函数的代数免疫阶,且该布尔函数是代数免疫阶最小的分量函数的非零非线性组合,从而得出多输出布尔函数的代数免疫阶等于其所有非零非线性组合代数免疫阶的最小值.该结论将多输出布尔函数的代数免疫问题转化为布尔函数的代数免疫问题.如何利用该性质解决多输出布尔函数代数免疫阶的快速计算问题以及具有高代数免疫阶的多输出函数的构造问题?有待我们进一步深入研究.

参考文献:

[1] N Courtois, W Meier. Algebraic attacks on stream ciphers with linear feedback[A]. Advances in Cryptology-EUROCRYPT 2003[C]. LNCS 2656, Berlin: Springer-Verlag, 2003. 345 – 359.

[2] N Courtois. Fast algebraic attacks on stream ciphers with linear feedback[A]. Advances in Cryptology-CRYPTO 2003[C]. LNCS 2729, Berlin: Springer-Verlag, 2003. 176 – 194.

[3] F Armknecht, M Krause. Algebraic attacks on combiners with memory[A]. Advances in Cryptology-CRYPTO 2003[C]. LNCS 2729. Berlin: Springer-Verlag, 2003: 162 – 175.

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

[5] D Dalai, K Gupta, S Maitra. Results on algebraic immunity for

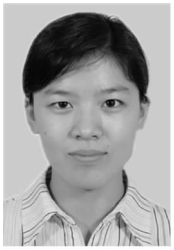
cryptographically significant Boolean functions[A]. Indocrypt 2004[C]. LNCS 3348. Berlin: Springer Verlag, 2004. 92 – 106.

[6] 张文英,武传坤.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. On the annihilators of cryptographic Boolean functions[J]. Acta Electronica Sinica, 2006, 34(1):51 – 54. (in Chinese)

[7] LI N, Qi W F. On the construction of Boolean functions with optimal algebraic immunity[J]. IEEE Transactions, 2008, 54(3):1330 – 1334.

[8] S Fischer, W Meier. Algebraic immunity of S-boxes and augmented functions[A]. Advances in FSE 2007[C]. LNCS 4593. Berlin: Springer Verlag, 2007. 366 – 381.

作者简介:



王秋艳　女,1985 年 3 月出生于江苏连云港,信息工程大学电子技术学院博士研究生,主要研究方向为密码学.
E-mail: wangqiuyan06@gmail.com

金晨辉　男,1965 年出生于河南扶沟,信息工程大学电子技术学院教授,博士生导师,主要研究方向为密码学和信息安全等.
E-mail: jinchenhui@126.com