基于 T-D 猜想上 MAI 函数的构造

张喆琳 周 梦
(北京航空航天大学数学与系统科学学院 LMIB 北京 100191)

摘 要 对涂自然等人提出的组合猜想上的构造方法及有关结论进行了改良推广,在假设更一般的组合猜想成立的前提下构造了一种具有最优代数免疫度的偶数元布尔函数 f,同时还利用 f 构造了一种具有最优代数免疫度的平衡的偶数元布尔函数 F。且这些函数也具有很高的代数次数和非线性度,对代数攻击具有较强的抵抗能力。

关键词 布尔函数,代数免疫度,平衡性,非线性度,代数次数
中图法分类号 TP309 **文献标识码** A

Construction of MAI Function Based on T-D Conjecture

ZHANG Zhe-lin ZHOU Meng
(School of Mathematics and System Science, LMIB, BeiHang University, Beijing 100191, China)

Abstract An improvement was made on the construction method and the relevant conclusions of combinatorial conjecture proposed by Ziran Tu. Under the premise that the more general combinatorial conjecture is still rational, a class of Boolean functions f with the maximum algebraic immunity on even number of variables was presented, and using the functions f, a new class of balanced Boolean functions F with the maximum algebraic immunity on even number of variables was gotten. These functions not only have higher algebraic degree and nonlinearity, but also have strong resistance against algebraic attacks.

Keywords Boolean functions, Algebraic immunity, Balancedness, Nonlinearity, Algebraic degree

1 引言

布尔函数在设计流密码(非线性滤波函数及非线性组合函数)和分组密码(如S盒)中有重要应用,其密码学性质的好坏直接关系到密码算法的安全性。为了保证密码系统有较强的保密功能,所使用的布尔函数必须满足一定的性质:如平衡性、对称性、相关免疫阶、高的代数次数、高的非线性度、扩散性和严格雪崩性等。2003年欧密会上,Courtois、Armknecht等人提出和发展了一种新的攻击方式——代数攻击,它成功地攻击了 Toyocrypt 和 LILI-1 28 等许多流密码算法,受到了密码学界的高度关注[1-4]。代数攻击的提出和发展被认为是密码分析技术中最重要的突破之一。为了抵抗代数攻击,Meier[5]等人引入度量布尔函数的新指标——代数免疫。代数免疫的提出给密码函数的分析和设计提出了新的课题。代数免疫也成为衡量布尔函数密码学性质的标准,因此,构造代数免疫度最优的布尔函数,成为了布尔函数研究的热点问题。

本文第2节介绍相关概念;第3节给出 T-D 猜想和相关新组合猜想;第4节给出了一类具有最优代数免疫度的偶数元布尔函数的构造,并讨论了它的代数次数和非线性度;第5节利用第4节中的结果给出了一类具有最优代数免疫度的平衡偶数元布尔函数的构造[6-13]。

2 预备知识

设 F_2 是二元有限域,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 元布尔函数的全体记作 B_n。一个 n 元布尔函数 f 的基本表示方法是真值表表示,即 F_2 上的一个长为 2^n 的向量:

$$(f(0,\cdots,0,0),f(0,\cdots,0,1),f(0,\cdots,1,0),\cdots,f(1,\cdots,1,1))$$

n 元布尔函数 f 的支撑集定义为 $supp(f)=\{x\in F_2^n \mid f(x)=1\}$。支撑集 $supp(f)$ 所含元素的个数称为 f 的 Hamming 重量,记为 $\omega t(f)$。若 $\omega t(f)=2^{n-1}$,则称 n 元布尔函数是平衡的。两个 n 元布尔函数 f 和 g 的 Hamming 距离定义为 $\omega t(f+g)$。

每一个 n 元布尔函数 f 还可以唯一地表示为 F_2 上的含 n 个变元的多项式,称之为 f 的代数正规型(Algebraic Normal Form, ANF):

$$f(x_1,\cdots,x_n)=\sum_{I\subset\{1,2,\cdots,n\}} a_I \prod_{i\in I} x_i \quad (a_I\in F_2)$$

非零布尔函数 f 的代数次数 $\deg(f)$ 定义为代数正规型中系数非零项所含最多变元的个数,即 $\deg(f)=\max_{I\subset\{1,2,\cdots,n\}}\{|I| \mid a_I\neq 0\}$。规定代数系数不超过1的布尔函数为仿射函数,全体 n 元仿射函数的集合记为 A_n。

到稿日期:2013-01-19 返修日期:2013-04-03 本文受国家自然科学基金(NSFC11271040)资助。
张喆琳(1988-),女,硕士生,主要研究方向为密码学,E-mail:zzhelin@126.com;周 梦(1958-),男,教授,博士生导师,主要研究方向为代数学及其应用、代数与符号计算、密码学理论。

设 F_{2^n} 为 2^n 元有限域，则它可以看成 F_2 上的 n 维向量空间。F_{2^n} 上的任意布尔函数也可以表示成唯一的单变元多项式：

$$f(x)=\sum_{i=0}^{2^n-1}a_i x^i$$

其中，$a_0, a_{2^n-1}\in F_2$，$a_i\in F_{2^n}$，$1\leqslant i<2^n-1$，且满足 $a_i^2=a_{2i(\bmod 2^n-1)}$。

f 的代数次数 $\deg(f)$ 为 $\max\{\omega t(\bar{i})\mid a_i\neq 0, 0\leqslant i<2^n\}$，这里 $\bar{i}$ 为 i 的二进制展开。

Hamming 距离：$d_H(f,g)=|\{x\in F_2^n\mid f(x)+g(x)=1\}|$。

非线性度：$nl(f)=\min_{g\in A_n}(d_H(f,g))$。

令 $x=(x_1,x_2,\cdots,x_n)$，$a=(a_1,a_2,\cdots,a_n)$ 都属于 F_2^n。记 $a\cdot x=a_1x_1+a_2x_2+\cdots+a_nx_n$，则 Walsh 谱 $W_f(a)=\sum_{x\in F_2^n}(-1)^{f(x)+a\cdot x}$。

对于 $f:F_{2^n}\to F_2$，其 f 在 a 点的 Walsh 谱定义为：

$$W_f(a)=\sum_{x\in F_{2^n}}(-1)^{f(x)+tr(ax)},\ a\in F_{2^n}$$

其中，tr 是从 F_2^n 到 F_2 上的迹函数：$tr(x)=x+x^2+x^{2^2}+\cdots+x^{2^{n-1}}$。

对于 $f:F_{2^k}\times F_{2^k}\to F_2$，其 f 在 (a,b) 点的 Walsh 谱定义为：

$$W_f(a,b)=\sum_{(x,y)\in F_{2^k}\times F_{2^k}}(-1)^{f(x,y)+tr(ax+by)},\ (a,b)\in F_{2^k}\times F_{2^k}$$

一个布尔函数 f 是平衡函数当且仅当 $W_f(0)=0$。f 的非线性度也可以由 Walsh 谱给出：

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

对任意 n 元布尔函数 f，有 $nl(f)\leqslant 2^{n-1}-2^{\frac{n}{2}-1}$。达到这个上界的布尔函数称为 Bent 函数。

对 $f\in B_n(x)$，f 的零化子的集合记作：

$Ann(f)=\{g\in B_n(x)\mid fg=0\}$

定义 1 布尔函数 f 的代数免疫度(Algebraic Immunity) $AI(f)$ 指的是：f 与 $f+1$ 的非零零化子的最低次数，即

$$AI(f)=\min\{\deg(g)\mid 0\neq g\in Ann(f)\cup Ann(f+1)\}$$

可以证明，n 元布尔函数的代数免疫度不超过 $\left\lceil\frac{n}{2}\right\rceil$[3,5]。

如果一个 n 元布尔函数的代数免疫度恰好等于 $\left\lceil\frac{n}{2}\right\rceil$，则称该函数具有最优代数免疫度或最大代数免疫度(Maximum Algebraic Immunity)，简称 MAI 函数。

3 组合猜想

受 Carlet 和冯克勤工作的启发，涂自然和邓映蒲首先给出了关于二进制字符串的一个组合猜想，并在假设此猜想成立的前提下证明了一类 PS 型 Bent 函数为 MAI 函数。

猜想 1[9] 设 $k\in Z, k>1$，对任意 $x\in Z_{2^k-1}$，把 x 展开成 k 位二进制数，用 $\omega t(\bar{x})$ 表示 x 的展开式中 1 的个数，对任意 $t\in Z, 0<t<2^k-1$，令

$$S_t=\{(a,b)\mid a,b\in Z_{2^k-1}, a+b\equiv t \bmod 2^k-1, \omega t(\bar{a})+\omega t(\bar{b})\leqslant k-1\}$$

则 $|S_t|\leqslant 2^{k-1}$。

虽然，到目前为止还无法给出一个精确的证明，但涂自然和邓映蒲已经验证了当 $k\leqslant 29$ 时此猜想的合理性。D. Tang 等人在文献[10]中又给出了一个类似的新组合猜想：

猜想 2[10] 设 $k\in Z, k>1$。对任意 $0<t<2^k-1$，定义

$$S_{t,-}=\{(a,b)\mid a,b\in Z_{2^k-1}, a-b\equiv t \bmod 2^k-1, \omega t(\bar{a})+\omega t(\bar{b})\leqslant k-1\}$$

则 $|S_{t,-}|\leqslant 2^{k-1}$。

同时，又给出一个一般化的猜想：

猜想 3[10] 设 $k\in Z, k>1, u\in Z_{2^k-1}^*$。对任意 $0<t<2^k-1$，定义

$$S_{t,u,-}=\{(a,b)\mid 0\leqslant a,b<2^k-1, ua-b\equiv t \bmod 2^k-1, \omega t(\bar{a})+\omega t(\bar{b})\leqslant k-1\}$$

则 $|S_{t,u,-}|\leqslant 2^{k-1}$。

并且，当 $2\leqslant k\leqslant 15$ 时，文献[10]对 $ua\pm b$ 的情况给出了验证。可见猜想 3 包括了猜想 2 这种特殊情况，下面将给出一个更一般化的组合猜想：

猜想 4 设 $k\in Z, k>1, u,v\in Z_{2^k-1}^*$。对任意 $0<t<2^k-1$，定义

$$S_{t,u,-v}=\{(a,b)\mid 0\leqslant a,b<2^k-1, ua-vb\equiv t \bmod (2^k-1), \omega t(\bar{a})+\omega t(\bar{b})\leqslant k-1\}$$

则 $|S_{t,u,-v}|\leqslant 2^{k-1}$。

引理 1 猜想 4 等价于猜想 3。

文献[11]中已证明了 $ua+vb$ 的情况等同于 $ua+b$ 的情况，这里也可以用同样的手段得到相应证明。

引理 2[10] 设 $k>1, k\in Z$，则 $|S_{t,-}|=|S_{2^k-1-t,-}|$，$0<t<2^{k-1}$。

4 最优代数免疫度的布尔函数

在这部分，假设猜想 4 成立的条件下，我们将构造一类代数免疫度最优的偶数元布尔函数，同时讨论它的代数次数和非线性度。这里仅给出最一般形式的构造：

构造 1 设 $n=2k\geqslant 4$，$(u,2^k-1)=1$。α 为 F_{2^k} 的本原元，设 $\Delta_s=\{\alpha^s,\alpha^{s+1},\cdots,\alpha^{s+2^{k-1}-1}\}$。其中 $0\leqslant s<2^k-1, s\in Z$。定义 $f\in B_n$ 如下：

$$f(x,y)=g(x^v y^u),\ (v,2^k-1)=1$$

其中，g 是定义在 F_{2^k} 上满足 $supp(g)=\Delta_s$ 的布尔函数。

4.1 代数免疫度

定理 1 设 f 是构造算法 1 中的 n 元布尔函数，若猜想 4 成立，则 f 具有最优代数免疫度，即 $AI(f)=k$。

证明：即证 f 和 $f+1$ 都没有代数次数低于 k 的非零零化子。令非零布尔函数 $h:F_{2^k}\times F_{2^k}\to F_2$ 满足 $\deg(h)<k$，并且 $f\cdot h=0$。下证 $h=0$。

由构造 1 知，

$$supp(f)=\{(\gamma^{1/v}y^{2^k-1-u}, y^v)\mid y\in F_{2^k}^*, \gamma\in\Delta_s\},$$

设

$$h(x,y)=\sum_{i=0}^{2^k-1}\sum_{j=0}^{2^k-1}h_{i,j}x^i y^j$$

$h_{i,j}\in F_{2^k}$ 是 f 的一个零化子，且 $\deg(h)<k$，即：

(1) $h(\gamma^{1/v}y^{2^k-1-u}, y^v)=0, \forall\, y\in F_{2^k}^*, \gamma\in\Delta_s$；

(2) 若 $\omega t(\bar{i})+\omega t(\bar{j})\geqslant k$，则 $h_{i,j}=0$。由此推出 $h_{2^k-1,j}=h_{i,2^k-1}=0, (0\leqslant i,j\leqslant 2^k-1)$。

则有

$$h(\gamma^{1/v}y^{2^k-1-u},y^v)=\sum_{i=0}^{2^k-2}\sum_{j=0}^{2^k-2}h_{i,j}\gamma^{\frac{1}{v}i}y^{vj-ui}$$
$$=\sum_{t=0}^{2^k-2}h_t(\gamma)y^t$$

令$\frac{1}{v}=w$,因为$(v,2^k-1)=1$,所以$w\in Z_{2^k-1}$,且$(w,2^k-1)=1$。其中

$$h_t(\gamma)=\sum_{0\leqslant i,j\leqslant 2^k-2,vj-ui\equiv t(\mathrm{mod}\,2^k-1)}h_{i,j}\gamma^{\frac{1}{v}i}$$
$$=h_{0,wt(\mathrm{mod}\,2^k-1)}+h_{1,w(t+u)(\mathrm{mod}\,2^k-1)}\gamma^w+h_{2,w(t+2u)(\mathrm{mod}\,2^k-1)}\gamma^{2w}+\cdots+h_{2^k-2,w(t+(2^k-2)u)(\mathrm{mod}\,2^k-1)}\gamma^{(2^k-2)w}$$

注:因为$(uw,2^k-1)=1$,所以$\{w(t+ui)(\mathrm{mod}\,2^k-1)\mid 0\leqslant i<2^k-1\}=Z_{2^k-1}$。

对$\forall\gamma\in\Delta_s$,由(1)得$h_t(\gamma)=0$,$0\leqslant t\leqslant 2^k-2$。再由BCH码的定义知,向量

$$(h_{0,wt(\mathrm{mod}\,2^k-1)},h_{1,w(t+u)(\mathrm{mod}\,2^k-1)},h_{2,w(t+2u)(\mathrm{mod}\,2^k-1)},\cdots,h_{2^k-2,w(t+(2^k-2)u)(\mathrm{mod}\,2^k-1)})$$

是F_{2^k}上以Δ_s中的元素为零点、设计距离为$2^{k-1}+1$、码长为2^k-1的一个BCH码。根据BCH界,我们知道,若这个码字非零,则它的Hamming重量至少为$2^{k-1}+1$。然而,由猜想4知它的Hamming重量不会超过2^{k-1}。这就导致了矛盾,因此这个码字必为零。即

$$h_{0,wt(\mathrm{mod}2^k-1)}=h_{1,w(t+u)(\mathrm{mod}2^k-1)}=h_{2,w(t+2u)(\mathrm{mod}2^k-1)}=\cdots=h_{2^k-2,w(t+(2^k-2)u)(\mathrm{mod}\,2^k-1)}=0$$

对$\forall 0\leqslant t\leqslant 2^k-2$成立,这就证明了$h=0$。

下面,我们类似证明$f+1$的情况。设$h(x,y)\in B_{2k}$,且满足$\deg(h)<k$,$(f+1)\cdot h=0$,同样要证明$h=0$。

$supp(f+1)=\{(x,y)\mid x^vy^u\in F_{2^k}\backslash\Delta_s,x,y\in F_{2^k}\}$

类似地,对$0\leqslant t\leqslant 2^k-2$,有

$h_t(\gamma)=0$,$\forall\gamma\in F_{2^k}^*\backslash\Delta_s$。

同时,$h(x,0)=0$。对所有的$x\in F_{2^k}$,有$h_{i,0}=0$,$0\leqslant i\leqslant 2^k-2$。向量

$$(h_{0,wt(\mathrm{mod}\,2^k-1)},h_{1,w(t+u)(\mathrm{mod}\,2^k-1)},h_{2,w(t+2u)(\mathrm{mod}\,2^k-1)},\cdots,h_{2^k-2,w(t+(2^k-2)u)(\mathrm{mod}2^k-1)})$$

也是F_{2^k}上一个以$F_{2^k}^*\backslash\Delta_s$中的元素为零点、设计距离为$2^{k-1}$、码长为$2^k-1$的BCH码。根据BCH界,我们知道,若这个码字非零,则它的Hamming重量大于等于2^{k-1}。然而,由猜想4和$h_{i,0}=0(0\leqslant i\leqslant 2^k-2)$,知它的Hamming重量严格小于$2^{k-1}$。矛盾产生,所以$h=0$。

通过以上讨论可知,f和$f+1$都没有代数次数低于k的非零零化子,所以$AI(f)=k$。这也意味着我们所构造的布尔函数具有最优代数免疫度。

4.2 多项式和代数次数

定理2 设f为构造1中的n元布尔函数,则它的二变元表示为:

$$f(x,y)=\sum_{i=1}^{2^k-2}\alpha^{-is}(1+\alpha^{-i})^{2^{k-1}-1}(x^vy^u)^i$$

因此,f的代数次数为$\max_{1\leqslant i\leqslant 2^k-2}\{\omega t(\overline{vi})+\omega t(\overline{ui})\}$,有$k\leqslant\deg(f)\leqslant 2(k-1)$。

证明:设$g(y)=\sum_{i=0}^{2^k-1}g_iy^i$为$g$的单变量表示,则$g_0=g(0)=0$。又由于$g$的Hamming重量为偶数,故代数次数至多为$k-1$,所以$g_{2^k-1}=0$。进一步,$\forall i\in\{1,\cdots,2^k-2\}$,

$$g_i=\sum_{j=0}^{2^k-2}g(\alpha^j)\alpha^{-ij}=\sum_{j=s}^{2^{k-1}-1+s}\alpha^{-ij}=\alpha^{-is}\frac{1+\alpha^{-i2^{k-1}}}{1+\alpha^{-i}}$$
$$=\alpha^{-is}(1+\alpha^{-i})^{2^{k-1}-1}$$

所以有$g(y)=\sum_{i=1}^{2^k-2}\alpha^{-is}(1+\alpha^{-i})^{2^{k-1}-1}y^i$。于是$g_{2^k-2}\neq 0$,$\deg(g)=k-1$。由$f(x,y)$的定义可知,

$$f(x,y)=g(x^vy^u)=\sum_{i=1}^{2^k-2}\alpha^{-is}(1+\alpha^{-i})^{2^{k-1}-1}(x^vy^u)^i$$

且$\deg(f)=\max_{1\leqslant i\leqslant 2^k-2}\{\omega t(\overline{vi})+\omega t(\overline{ui})\}$。显然$k\leqslant\deg(f)\leqslant 2(k-1)$。

注:在定理2中,因为u,v都与2^k-1互素,所以$\omega t(\overline{ui})\geqslant 1$,$\omega t(\overline{vi})\geqslant 1$,当$u\neq v$时,对固定的$v$,一定存在一个$i'$,使得$vi'=2^k-2$,所以$\deg(f)\geqslant\omega t(\overline{vi'})+\omega t(\overline{ui'})\geqslant k$;当$u=v$时,$\deg(f)=\max_{1\leqslant i\leqslant 2^k-2}\{2\omega t(\overline{ui})\}=2(k-1)=n-2$。

4.3 非线性度

引理3 设$k\in Z,k\geqslant 2$。α为F_{2^k}上的一个本原元。记$\Delta_s=\{\alpha^s,\alpha^{s+1},\cdots,\alpha^{s+2^{k-1}-1}\}$,$0\leqslant s<2^k-1$,$s\in Z$。定义

$$\Gamma_s=\sum_{r\in\Delta_s}\sum_{x\in F_{2^k}^*}(-1)^{tr(1/x+rx^u)}$$

其中,$(u,2^k-1)=1$,则

$$|\Gamma_s|\leqslant 1+\frac{2^{k+1}}{\pi}\ln\frac{4(2^k-1)}{\pi}$$

证明:设$\zeta=e^{\frac{2\pi\sqrt{-1}}{2^k-1}}$是复数域上$2^k-1$次本原单位根。令$\chi$是$F_{2^k}^*$上的乘法特征标,定义为$\chi(\alpha^j)=\zeta^j$($0\leqslant j\leqslant 2^k-2$)且$\chi(0)=0$。定义高斯和如下:

$$G(\chi^\mu)=\sum_{x\in F_{2^k}^*}\chi^\mu(-1)^{tr(x)},0\leqslant\mu\leqslant 2^k-2$$

由文献[12]我们清楚地知道$G(\chi^0)=-1$,$|G(\chi^\mu)|=2^{\frac{k}{2}}$($1\leqslant\mu\leqslant 2^k-2$)。通过傅里叶变换,有

$$(-1)^{tr(\alpha^j)}=\frac{1}{2^k-1}\sum_{\mu=0}^{2^k-2}G(\chi^\mu)\overline{\chi^\mu}(\alpha^j),0\leqslant j\leqslant 2^k-2。$$

记$q=2^k$,则有

$$\Gamma_s=\sum_{r\in\Delta_s}\sum_{j=0}^{q-2}(-1)^{tr(\alpha^{-j})}(-1)^{tr(r\alpha^{uj})}$$
$$=\frac{1}{(q-1)^2}\sum_{i=s}^{\frac{q}{2}+s-1}\sum_{j=0}^{q-2}\sum_{\mu,\nu=0}^{q-2}G(\chi^\mu)G(\chi^\nu)\chi^{\mu j-\nu(i+uj)}$$
$$=\frac{1}{(q-1)^2}\sum_{\mu,\nu=0}^{q-2}G(\chi^\mu)G(\chi^\nu)(\sum_{i=s}^{\frac{q}{2}+s-1}\zeta^{-\nu i})(\sum_{j=0}^{q-2}\zeta^{(\mu-u\nu)j})$$

容易推出

$$\sum_{i=s}^{\frac{q}{2}+s-1}\zeta^{-\nu i}=\zeta^{-\nu s}\sum_{i=0}^{\frac{q}{2}-1}\zeta^{-\nu i}=\begin{cases}\frac{q}{2}, & \nu=0\\ \zeta^{-\nu s}\frac{1-\zeta^{-\nu\frac{q}{2}}}{1-\zeta^{-\nu}}, & \nu\neq 0\end{cases}$$

且

$$\sum_{j=0}^{q-2}\zeta^{(\mu-u\nu)j}=\begin{cases}q-1, & \mu=\nu u\\ 0, & \mu\neq\nu u\end{cases}$$

因此

$$\Gamma_s=\frac{q}{2(q-1)}+\frac{1}{q-1}\sum_{\nu=1}^{q-2}G(\chi^{\nu u})G(\chi^\nu)(\zeta^{-\nu s}\frac{1-\zeta^{-\nu\frac{q}{2}}}{1-\zeta^{-\nu}})$$
$$=\frac{q}{2(q-1)}+\frac{1}{q-1}\sum_{\nu=1}^{q-2}G(\chi^{\nu u})G(\chi^\nu)(\zeta^{-\nu s+\frac{\nu}{2}-\frac{\nu q}{4}}\frac{\zeta^{\frac{\nu q}{4}}-\zeta^{-\frac{\nu q}{4}}}{\zeta^{\frac{\nu}{2}}-\zeta^{-\frac{\nu}{2}}})$$

$$=\frac{q}{2(q-1)}+\frac{1}{q-1}\sum_{\nu=1}^{q-2}G(\chi^{\nu u})G(\chi^{\nu})(\zeta^{-us+\frac{\nu}{2}-\frac{u\pi}{4}}\frac{\sin\frac{\nu q\pi}{2(q-1)}}{\sin\frac{\nu\pi}{q-1}})$$

进而有

$$|\Gamma_s|\leqslant\frac{q}{2(q-1)}+\frac{1}{q-1}\sum_{\nu=1}^{q-2}|G(\chi^{\nu u})||G(\chi^{\nu})|(\frac{1}{|\sin\frac{\nu\pi}{q-1}|})$$

$$=\frac{q}{2(q-1)}+\frac{q}{q-1}\sum_{\nu=1}^{q-2}(\frac{1}{\sin\frac{\nu\pi}{q-1}})$$

由文献[13]知，$\sum_{\nu=1}^{q-2}(\sin\frac{\nu\pi}{q-1})^{-1}\leqslant-\frac{2(q-1)}{\pi}\ln\tan(\frac{\pi}{4(q-1)})$，所以可得

$$|\Gamma_s|\leqslant\frac{q}{2(q-1)}-\frac{2q}{\pi}\ln\tan(\frac{\pi}{4(q-1)})\leqslant1-\frac{2q}{\pi}\ln\frac{\pi}{4(q-1)}$$
$$\leqslant1+\frac{2q}{\pi}\ln\frac{4(q-1)}{\pi}$$

因此，得出了$|\Gamma_s|\leqslant1+\frac{2^{k+1}}{\pi}\ln\frac{4(2^k-1)}{\pi}$。

定理3 设$n=2k$，$f\in B_n$为构造1中的n元布尔函数。则有

$$nl(f)\geqslant2^{n-1}-\frac{2^{k+1}}{\pi}\ln\frac{4(2^k-1)}{\pi}-1\approx2^{n-1}-\frac{2\ln2}{\pi}k2^k$$

证明：我们仅需计算$W_f(a,b)$。因为$\omega t(f)=(2^k-1)\cdot2^{k-1}=2^{2k-1}-2^{k-1}$，显然$W_f(0,0)=2^k$。

对$\forall(a,b)\in F_{2^k}\times F_{2^k}\backslash\{(0,0)\}$，有

$$W_f(a,b)=\sum_{(x,y)\in F_{2^k}\times F_{2^k}}(-1)^{f(x,y)+tr(ax+by)}$$
$$=-2\sum_{(x,y)\in supp(f)}(-1)^{tr(ax+by)}$$
$$=-2\sum_{r\in\Delta_s}\sum_{x\in F_{2^k}^*}(-1)^{tr(ax+br^{\frac{1}{w}}/x^{\frac{1}{u}})}$$
$$=-2\sum_{r\in\Delta_s}\sum_{x\in F_{2^k}^*}(-1)^{tr(ax^u+br^{\frac{1}{w}}/x)}$$
$$=\begin{cases}-2\sum_{r\in\Delta_s}\sum_{x\in F_{2^k}^*}(-1)^{tr(br^{\frac{1}{w}}/x)} & a=0,b\in F_{2^k}^*\\ -2\sum_{r\in\Delta_s}\sum_{x\in F_{2^k}^*}(-1)^{tr(ax^u)} & b=0,a\in F_{2^k}^*\\ -2\sum_{r\in\Delta_s}\sum_{x\in F_{2^k}^*}(-1)^{tr(1/x+ab^ur^{\frac{u}{v}}x^u)} & a\in F_{2^k}^*,b\in F_{2^k}^*\end{cases}$$

由$(u,2^k-1)=1$，$1+\sum_{x\in F_{2^k}^*}(-1)^{tr(ax^u)}=1+\sum_{x\in F_{2^k}^*}(-1)^{tr(br^{\frac{1}{w}}/x)}=0$，得

$$W_f(a,b)=\begin{cases}2^k, & a=0,b\in F_{2^k}^*\\ 2^k, & b=0,a\in F_{2^k}^*\\ -2\sum_{r\in\Delta_s}\sum_{x\in F_{2^k}^*}(-1)^{tr(1/x+ab^ur^{\frac{u}{v}}x^u)}, & a\in F_{2^k}^*,b\in F_{2^k}^*\end{cases}$$

由此可推出

$$\max_{(a,b)\in F_{2^k}^*\times F_{2^k}^*}|W_f(a,b)|$$
$$=\max\{-2\max_{0\leqslant s<2^k-1}|\sum_{r\in\Delta_s}\sum_{x\in F_{2^k}^*}(-1)^{tr(1/x+rx^u)}|,2^k\}$$

再由引理3有

$$nl(f)=2^{n-1}-\frac{1}{2}\max_{(a,b)\in F_{2^k}^*\times F_{2^k}^*}|W_f(a,b)|$$
$$\geqslant2^{n-1}-(1+\frac{2^{k+1}}{\pi}\ln\frac{4(2^k-1)}{\pi})$$
$$\approx2^{n-1}-\frac{2\ln2}{\pi}k2^k$$

通过以上证明计算，我们发现在假设猜想4和文献[11]中更一般化的猜想成立的条件下所构造的布尔函数具有相同性质。这说明关于此类猜想下布尔函数的构造，我们可以得到一个公共的普遍性结论。

表1中给出了当n很小时，文献[10]中特殊构造和定理3中的一般性构造的非平衡布尔函数非线性度下界值的对照，可以看出我们的结果适于此类猜想下构造的所有函数的情形，是由特殊到一般的转化。

表1 已知非线性度下界值的比较

n	上界$2^{n-1}-2^{n/2-1}$	文献[10]中的nl(f)	定理3中的nl(f)
6	28	22	21
8	120	106	99
10	496	462	441
12	2016	1935	1878
14	8128	7939	7796
16	32640	32208	31864

5 具有最优代数免疫度的平衡布尔函数

在这部分，我们将对构造1中的布尔函数进行改进得到一个平衡布尔函数。对于改进方法，我们采用文献[11]的手段(也可以用文献[10]的构造方法)。

构造2 设$n=2k,k\geqslant2$，α为有限域F_{2^k}上的一个本原元。记$\Delta_s=\{\alpha^s,\alpha^{s+1},\cdots,\alpha^{s+2^{k-1}-1}\}$，$0\leqslant s<2^k-1$。构造布尔函数$F\in B_n$如下：

$$F(x,y)=\begin{cases}g(x^vy^u), & x\neq0\\ g(y), & x=0\end{cases}$$

式中，g是F_{2^k}上满足$supp(g)=\Delta_s$的一个布尔函数。

经计算，我们发现也会得到类似文献[11]所构造的平衡布尔函数的一系列性质：构造算法2中得到的n元布尔函数F为平衡函数，其最大的代数次数为$n-1$，若新猜想4成立，则其最优代数免疫度为$AI(F)=n/2=k$。

同时我们可以计算出它的非线性度：

$$nl(f)\geqslant2^{n-1}-\frac{2\ln2}{\pi}k2^k-\frac{2\ln2}{\pi}k2^{\frac{k}{2}}$$

构造2中的这类布尔函数在$v=1,u=2^k-2$时，是Tu-Deng平衡函数[9]；在$v=u=1$时，是Tang提出的平衡函数[10]。

表2 平衡偶数元布尔函数非线性度下界值的对照

n	上界$2^{n-1}-2^{n/2-1}$	文献[9]中的nl(f)	文献[10]中的nl(f)	构造2的nl(f)
6	28	21	20	17
8	120	107	102	92
10	496	475	458	428
12	2016	1981	1929	1857
14	8128	8072	7931	7761
16	32640	32550	32195	31808

从表2也能看出，对于平衡偶数元布尔函数，构造2中的

(下转第111页)

本文采用均方根误差(RMSE)和平均相对误差(MAPE)两项性能指标来评判预测模型的性能。RMSE 和 MAPE 值越小,对应的模型预测性能越好。这 3 种模型的性能对比如表 1 所列。

表 1　3 种模型的性能对比

预测模型	RMSE	MAPE
IHS_RELM	0.024193	0.52617
Elman	0.049287	0.58374
HHGA_RBFNN	0.050416	0.60159

从表 1 中可以看出,IHS_RELM 预测模型的 RMSE 和 MAPE 值均小于其他两种模型的 RMSE 和 MAPE 值,表明 IHS_RELM 模型的预测性能优于其他两种模型。

结束语　对网络安全态势进行预测是主动防御黑客攻击的一种有效手段,有助于网络管理人员把握未来网络安全态势的发展趋势,从而提前采取相应的网络安全措施。本文提出一种基于 IHS_RELM 的网络安全态势预测方法,其将 RELM 嵌入到 IHS 算法的适应度计算过程中,利用 IHS 算法的全局搜索能力来优化选取 RELM 的输入权值和隐含层阈值,在一定程度上提升了 RELM 的学习能力和泛化能力。仿真实验结果表明,该方法对于预测未来的网络安全态势值具有较好的效果。

下一步的研究工作:

1. 如何获取 RELM 算法中最佳的隐含层节点数,期望获取更好的模型结构;

2. 如何将 IHS_RELM 算法与在线学习算法结合起来,期望实现实时网络安全态势预测。

参 考 文 献

[1] Zhang Song-mei, Yao Shan, Ye Xin'en, et al. A Network Security Situation Analysis Framework Based on Information Fusion [C]// Information Technology and Artificial Intelligence Conference(ITAIC). 2011 6th IEEE Joint International. 2011, 1: 326-332

[2] 韩敏娜,刘渊,陈烨. 基于集对分析的网络安全态势评估[J]. 计算机应用研究,2012,29(10):3824-3827

[3] 孟锦,马驰,何加浪,等. 基于 HHGA-RBF 神经网络的网络安全态势预测模型[J]. 计算机科学,2011,38(7):71-75

[4] 尤马彦,凌捷,郝彦军. 基于 Elman 神经网络的网络安全态势预测方法[J]. 计算机科学,2012,39(6):61-76

[5] 王晋东,沈柳青,王坤,等. 网络安全态势预测及其在智能防护中的应用[J]. 计算机应用,2010,30(6):1480-1488

[6] 邓万宇,郑庆华,陈琳,等. 神经网络极速学习方法研究[J]. 计算机学报,2010,33(2):279-287

[7] Geem Z W, Kim J H, Loganathan G V. A new heuristic optimiza-tion algorithm: harmony search[J]. Simulation, 2001, 76(2): 60-68

[8] Omran M G H, Mahdavi M. Global-best Harmony Search[J]. Applied Mathematics and Computation, 2008, 198(2): 643-656

[9] 周江嫚,黄清秀,彭敏放,等. 基于差分进化优化 ELM 的模拟电路故障诊断[Z]. 计算机工程与应用,2012

[10] Honeynet Project. Know Your Enemy: Statistics[EB/OL]. http://old.honeynet.org/papers/stats/, 2001

[11] 陈秀真,郑庆华,管晓宏,等. 层次化网络安全威胁态势量化评估方法[J]. 软件学报,2006,17(4):885-897

(上接第 97 页)

$nl(f)$的下界范围更广了。所以构造 2 中的函数不仅在形式上具有普遍性,性质上也同样具有一般性。

结束语　本文给出了一种具有最优代数免疫度的偶数元布尔函数的构造,并且还给出了一种具有最优代数免疫度的平衡偶数元布尔函数的构造。因为猜想 4 和猜想 3 等价,我们也可以从猜想 3 的角度出发进行较特殊情况的构造,用 xy^u 代替 x^vy^u,经计算证明发现也可得到相同结果,且计算更简便。本文中还存在一些亟待解决的问题,比如当 u,v 为何值时,构造 1 中的函数为 Bent 函数;所构造函数与其它已知函数性质的比较等等,都是我们下一步要研究的重点。

参 考 文 献

[1] Armknecht F. Improving fast algebraic attacks: FSE 2004[C]// LNCS 3017. Springer Verlag, 2004: 65-82

[2] Batten L M. Algebraic attacks over GF(q): Cryptology-INDOCRYPT 2004[C]// LNCS 3348. Springer Verlag, 2004: 84-91

[3] Courtois N, Meier W. Algebraic attacks on stream ciphers with linear feedback: Cryptology-EUROCRYPT 2003[C]// LNCS 2656. Springer Verlag, 2003: 345-359

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

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

[6] 孟强,陈鲁生,符方伟. 一类代数免疫度达到最优的布尔函数的构造[J]. 软件学报,2010: 1758-1767

[7] 涂自然,邓映蒲. 代数免疫度为 1 的布尔函数[J]. 系统科学与数学,2011,31(5): 512-518

[8] 李超,薛朝红,付绍静. 代数免疫度最优的旋转对称布尔函数的构造[J]. 国防科技大学学报,2012,34(2): 34-38

[9] Tu Z, Deng Y. A conjecture about binary strings and its applications on constructing Boolean functions with optimal algebraic immunity: Des[J]. Codes Cryptogr, 2011, 60(1): 1-14

[10] Tang D, Carlet C, Tang X. Highly nonlinear Boolean functions with optimum algebraic immunity and good behavior against fast algebraic attacks[J]. Cryptology ePrint Archive, 2013, 59(1): 653-664

[11] Jin Q, Liu Z, Wu B, et al. A general conjecture similar to T-D conjecture and its applications in constructing Boolean functions with optimal algebraic immunity[C]// Cryptology ePrint Archive 2011. 2011: 515

[12] Lidl R, Niederreiter H. Finite Fields, Encyclopedia of Mathematics and its Applications[M]. 1983

[13] Carlet C, Feng K. An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity: Asiacrypt 2008[C]// LNCS 5350. SpringernVerlag, 2008: 425-440