m 阶相关免疫函数的构造和计数

郑浩然,金晨辉
(解放军信息工程大学电子技术学院,河南郑州 450004)

摘 要: 若布尔函数的输出不泄漏其输入值的有关信息,则称该函数是相关免疫的.这类函数在计算机保密应用中用途广泛.本文研究了 m 阶相关免疫函数的构造和计数问题,给出了两种新的构造方法.进一步,将这两种新构造方法与 Seigenthaler,杨义先,Camion,Seberry 以及温巧燕等人的构造方法进行了比较,证明了本文中的构造方法实际上推广了这些文献中的结论.利用本文中的构造方法,既可直接构造任意阶的相关免疫函数,又可根据已知的相关免疫函数来构造新的相关免疫函数.另外,基于新的构造方法,改进了 m 阶相关免疫的平衡函数的计数下界.

关键词: 布尔函数; 相关免疫; 平衡函数; 列平衡矩阵
中图分类号: TN918.1 **文献标识码**: A **文章编号**: 0372-2112 (2008) 04-0804-05

Construction and Enumeration of mth-Order Correlation Immune Functions

ZHENG Hao-ran, JIN Chen-hui
(*Institute of Electronic Technology, the PLA Information Engineering University, Zhengzhou, Henan* 450004, *China*)

Abstract: A Boolean function is said to be correlation immune if its output leaks no information about its input values. Such functions have extensive applications in computer security practices. This paper studies the construction and enumeration problem for mth-order correlation immune functions and presents two new construction methods. Furthermore, we compare new methods with Seigenthaler, Yang, Camion, Seberry, Wen et al's and show that new methods actually generalize relational conclusions in these references. Using new methods not only can construct directly mth-order correlation-immune functions, but also can construct new correlation immune functions on the basis of known correlation immune functions. In addition, based on new construction methods, the enumeration lower bound of balanced mth-order correlation immune functions is improved.

Key words: Boolean function; correlation immunity; balanced function; column-balanced matrix

1 引言

相关免疫函数是 Seigenthaler 在 1984 年研究流密码系统的安全性时提出的,它在计算机保密应用中用途广泛.前馈网络中的非线性组合函数如果泄漏了其输入的有关信息,就会大大降低攻击该密码体制所需的工作量,而相关免疫函数能够有效地抵抗这种相关攻击;另外,相关免疫函数和正交矩阵是等价的,而正交矩阵是研究认证码的重要工具,这就使得我们可通过构造相关免疫函数来构造正交矩阵,进而设计出好的认证码.因此,寻求相关免疫函数的简单构造方法并研究其计数下界具有十分重要的意义.

Siegenthaler 在文献[1]中给出了一种构造相关免疫函数的方法,他给出的方法实质上是递归的,因此在实际应用中并非十分满意;杨义先等人在文献[2]中用重量分析方法研究相关免疫函数,给出了一些构造方法,讨论了两个布尔函数之和的相关免疫性;Camion 等人在文献[3]中从代数编码理论的角度对相关免疫函数进行了研究,提出了一种构造任意阶平衡相关免疫函数的方法;Seberry 等人在文献[4]中认为,利用文献[3]中的方法所构造的相关免疫函数的非线性性和扩散特性无法讨论,于是该文通过 Hadamard 矩阵理论研究相关免疫函数,给出了一种直接构造任意阶平衡相关免疫函数的方法,并证明了利用该方法所构造的相关免疫函数的集合与用文献[3]中的方法所构造的相关免疫函数的集合完全一样,且认为该构造方法与文献[3]中的构造方法相比有一定的优越性;冯登国等人在文献[5]中讨论了利用文献[3]中的方法所构造的相关免疫函数的非线性性和扩散特性,并据此认为,文献[4]中的构造方法与文献[3]中的构造方法相比并无多少优点;温巧燕等人在文献[6]中通过矩阵方法研究相关免疫函数,给出了两个结构定理,并给出了 n 元 m 阶相关免疫的平衡函数个数 $N^{(m)}(2^{n-1}, n)$ 的一个下界

$$N^{(m)}(2^{n-1}, n) \geq C_2^{2^{n-m-1}} + C_2^{2^{n-m-1}} \sum_{j=2}^{n-m-1} C_{2^{j-1}}^{2^{j-2}} \cdot (C_{2^j}^{2^{j-1}})^{n-m-j} \cdot C_{2^{n-m-1}-2^{j-1}}^{2^{n-m-1}-2^j}$$

其中 C_n^m 表示从 n 个元素中取出 m 个元素的组合数.

本文讨论了相关免疫函数的构造和计数问题,给出了新的构造这类函数的方法,推广了文献[1~4,6]中的相应结论,改进了 m 阶相关免疫平衡函数的计数下界.

2 预备知识

为方便起见,本文将所有布尔函数都看作 0 阶相关

收稿日期:2004-04-05;修回日期:2008-03-01

免疫函数;将布尔常函数 $f(x)\equiv c$(c 为 0 或 1)看作任意阶相关免疫函数.

Siegenthaler 在文献[1]中给出相关免疫函数的定义如下:

定义 1　设 $x_1,\cdots,x_n$ 是 n 个相互独立且服从均匀分布的二元随机变量,n 元布尔函数 $f(x_1,\cdots,x_n)$ 称为 m 阶相关免疫的当且仅当对任意 $1\le i_1<\cdots<i_m\le n$ 和 $a_1,\cdots,a_m$ 成立

$$P[f(x_1,\cdots,x_n)=1\mid x_{i_1}=a_1,\cdots,x_{i_m}=a_m]=P[f(x_1,\cdots,x_n)=1]$$

该文中提出了相关免疫函数的一种递归构造方法.

构造方法 1:设 $f_1(x_1,\cdots,x_n)$ 和 $f_2(x_1,\cdots,x_n)$ 均为 m 阶相关免疫函数,且

$$P[f_1(x_1,\cdots,x_n)=1]=P[f_2(x_1,\cdots,x_n)=1]=p$$

则 $n+1$ 元布尔函数

$$f(x_1,\cdots,x_n,x_{n+1})=f_1(x_1,\cdots,x_n)\oplus x_{n+1}\oplus f_2(x_1,\cdots,x_n)(1\oplus x_{n+1})$$

也是 m 阶相关免疫函数,且

$$P[f(x_1,\cdots,x_n,x_{n+1})=1]=p$$

杨义先等人在文献[2]中讨论了两个布尔函数之和的相关免疫性,给出了如下结论.

结构定理 1　设 $f(x_1,\cdots,x_{n_1},y_1,\cdots,y_{n-n_1})=f_1(x_1,\cdots,x_{n_1})\oplus f_2(y_1,\cdots,y_{n-n_1})$,其中 $f_1(\cdot)$,$f_2(\cdot)$ 分别是 m_1,m_2 阶相关免疫的平衡函数,则 $f(\cdot)$ 是 m_1+m_2+1 阶相关免疫函数.

Camion 等人在文献[3]中给出一种直接构造平衡相关免疫函数的方法.

构造方法 2:设 $0<n_1<n$,$g(y)$ 和 $p_j(y)$,$j=1,\cdots,n_1$ 均为 $n-n_1$ 维布尔函数,令 $x=(x_1,\cdots,x_{n_1})$,则

$$f(x,y)=\bigoplus_{j=1}^{n_1}x_j p_j(y)\oplus g(y)$$

是 m 阶相关免疫的平衡函数,其中

$$m=\min\{w(p_1(y),\cdots,p_{n_1}(y))\mid y\in\{0,1\}^{n-n_1}\}-1$$

Seberry 等人在文献[4]中给出一个与文献[3]中的方法等价的构造方法.

设 n 和 n_1 是正整数($n>n_1$),记 $x=(x_1,\cdots,x_{n_1})\in\{0,1\}^{n_1}$,$y=(y_1,\cdots,y_{n-n_1})\in\{0,1\}^{n-n_1}$,$(x,y)=(x_1,\cdots,x_{n_1},y_1,\cdots,y_{n-n_1})\in\{0,1\}^n$,$\delta=(\delta_1,\cdots,\delta_{n-n_1})\in\{0,1\}^{n-n_1}$. 定义 $\{0,1\}^{n-n_1}$ 上的函数 $D_\delta(y)=(y_1\oplus\delta_1)\cdots(y_{n-n_1}\oplus\delta_{n-n_1})$;$\{0,1\}^{n_1}$ 上的函数 $\phi_\delta(x)=\langle r_\delta,x\rangle$,其中 $r_\delta\in\{0,1\}^{n_1}$,$\langle\cdot,\cdot\rangle$ 表示点积.

Seberry 等人具体构造如下:

构造方法 3:设 $0<n_1<n$,$g(y)$ 是 $n-n_1$ 维布尔函数,则

$$f(x,y)=\bigoplus_{\delta\in\{0,1\}^{n-n_1}}D_\delta(y)\phi_\delta(x)\oplus g(y)$$

是 m 阶相关免疫的平衡函数,其中

$$m=\min\{w(r_\delta)\mid\delta\in\{0,1\}^{n-n_1}\}-1$$

定义 2　设 A 是一个 ω 行 n 列的矩阵,称 A 是一个 $(\omega,n,2,m)$($m\le n$)正交矩阵,是指 A 的任 m 列构成的矩阵的行向量中,$GF(2)^m$ 中每个向量都出现且出现的次数相同.

定义 3　设 $f(x)=f(x_1,\cdots,x_n)$ 是 n 元布尔函数,$D=\{(d_1,\cdots,d_n)\in\{0,1\}^n\mid f(d_1,\cdots,d_n)=1\}$,称以 D 中所有向量为行向量组成的矩阵(不考虑行向量的顺序)C_f 为 $f(x)$ 的特征矩阵,亦称 $f(x)$ 为 C_f 的特征函数.

显然,布尔函数与其特征矩阵是一一对应的.

引理 1[7]　n 元布尔函数 $f(x)$ 是 m 阶相关免疫函数当且仅当 $f(x)$ 的特征矩阵 C_f 是 $(\omega,n,2,m)$ 正交矩阵.

显然,研究相关免疫函数和研究正交矩阵是等价的.

为了叙述方便,下面对布尔函数 $f(x)$ 和其特征矩阵 C_f 不加区别;对重量为 ω 的 n 元 m 阶相关免疫函数和其对应的 $(\omega,n,2,m)$ 正交矩阵不加区别.

约定:$\mathbf{1}=(1,\cdots,1)^{\mathrm{T}}$,$\mathbf{0}=(0,\cdots,0)^{\mathrm{T}}$,其中 T 表示转置;矩阵 $\bar{\mathrm{A}}$ 表示以 $GF(2)^n$ 中除去 $\omega\times n$ 矩阵 A 的行以外的所有向量为行构成的 $(2^n-\omega)\times n$ 矩阵.

显然,若 A 是 $(\omega,n,2,m)$ 正交矩阵,则 $\bar{\mathrm{A}}$ 是 $(2^n-\omega,n,2,m)$ 正交矩阵.

温巧燕等人在文献[6]中首先给出一个与文献[1]中的方法等价的结构定理.

结构定理 2　设 A,B 是 $(\omega,n,2,m)$ 正交矩阵,则 $C=\begin{bmatrix}\mathbf{1}&\mathrm{A}\\ \mathbf{0}&\mathrm{B}\end{bmatrix}$ 是 $(2\omega,n+1,2,m)$ 正交矩阵.

其次给出一个由 m 阶相关免疫函数构造 $m+1$ 阶相关免疫函数的方法.

结构定理 3　设 A 是 $(2^{n-1},n,2,m)$ 正交矩阵,则 $C=\begin{bmatrix}\mathbf{1}&\mathrm{A}\\ \mathbf{0}&\bar{\mathrm{A}}\end{bmatrix}$ 是 $(2^n,n+1,2,m+1)$ 正交矩阵.

结构定理 3 实际上是结构定理 1 当 $f_1(\cdot)=x_1\oplus 1$(此时 $m_1=0$)时的特殊情况.

3　相关免疫函数的构造

引理 2　设 $0<n_1<n$,若 $\forall\delta\in\{0,1\}^{n-n_1}$,$n_1$ 元函数 $f(x,\delta):\{0,1\}^{n_1}\to\{0,1\}$ 均满足 $P[f(x,\delta)=1]=p$,则 n 元函数 $f(x,y)$ 亦满足 $P[f(x,y)=1]=p$.

证明　因 $\forall\delta\in\{0,1\}^{n-n_1}$,均有 $P[f(x,\delta)=1]=p$,故 $\forall\delta\in\{0,1\}^{n-n_1}$,有 $w(f(x,\delta))=2^{n_1}\cdot p$,则

$$w(f(x,y))=\sum_{\delta\in\{0,1\}^{n-n_1}}w(f(x,\delta))=\sum_{\delta\in\{0,1\}^{n-n_1}}2^{n_1}\cdot p=2^{n_1}\cdot p\cdot 2^{n-n_1}=2^n\cdot p$$

故 $P[f(x,y)=1]=w(f(x,y))/2^n=p$.

在引理 2 中,若取 $p=1/2$,则有

推论 1[8] 设 $0<n_1<n$,如果 $\forall\delta\in\{0,1\}^{n-n_1}$,$f(x,\delta):\{0,1\}^{n_1}\to\{0,1\}$都是 n_1 元平衡函数,则 $f(x,y)$ 是 n 元平衡函数.

定理 1 设 $0<n_1<n$,$\forall\delta\in\{0,1\}^{n-n_1}$,$\varphi_\delta(x):\{0,1\}^{n_1}\to\{0,1\}$都是 $m(0\le m\le n_1)$阶相关免疫函数且有 $P[\varphi_\delta(x)=1]=p(p$ 为常数$)$,则 $f(x,y)=\varphi_y(x)$ 也是 m 阶相关免疫函数且有 $P[f(x,y)=1]=p$.

证明 设 $r\le m$,任取

$$1\le i_1<\cdots<i_r\le n_1,1\le j_1<\cdots<j_{t-r}\le n-n_1$$

任意固定

$$x_{i_1}=a_1,\cdots,x_{i_r}=a_r;y_{j_1}=b_1,\cdots,y_{j_{m-r}}=b_{m-r}$$

则对任意固定的 δ,由 $\varphi_\delta(x)$ 是 m 阶相关免疫函数知,$\varphi_\delta(x)$ 必是 r 阶相关免疫函数,从而有

$$P[\varphi_\delta(x)=1|\ x_{i_1}=a_1,\cdots,x_{i_r}=a_r]=P[\varphi_\delta(x)=1]=p$$

于是,对满足 $y_{j_1}=b_1,\cdots,y_{j_{m-r}}=b_{m-r}$ 的给定 $y\in\{0,1\}^{n-n_1}$,有

$$P[\varphi_y(x)=1|\ x_{i_1}=a_1,\cdots,x_{i_r}=a_r]=p$$

故由引理 2 知,在限定 $x_{i_1}=a_1,\cdots,x_{i_r}=a_r;y_{j_1}=b_1,\cdots,y_{j_{m-r}}=b_{m-r}$ 的条件下,亦有

$$P[f(x,y)=\varphi_y(x)=1]=p$$

即

$$P[f(x,y)=1|\ x_{i_1}=a_1,\cdots,x_{i_r}=a_r;\ y_{j_1}=b_1,\cdots,y_{j_{m-r}}=b_{m-r}]=p$$

又因为

$$\begin{aligned}P[f(x,y)=1]&=\#\{(x,y):f(x,y)=1\}/2^n\\&=\left(\sum_{y\in\{0,1\}^{n_1}}\#\{x:\varphi_y(x)=1\}\right)/2^n\\&=\left(\sum_{y\in\{0,1\}^{n_1}}2^{n_1-1}\right)/2^n=p\end{aligned}$$

故有

$$P[f(x,y)=1|\ x_{i_1}=a_1,\cdots,x_{i_r}=a_r;\ y_{j_1}=b_1,\cdots,y_{j_{m-r}}=b_{m-r}]=P[f(x,y)=1]=p$$

即 $f(x,y)=\varphi_y(x)$ 是 m 阶相关免疫函数,且 $P[f(x,y)=1]=p$.

注:在定理 1 中取 $n=n_1+1$ 即得文献[1]中的构造方法 1 和文献[6]中的结构定理 2.

由于 n 阶相关免疫的 n 元布尔函数是常值函数,故 n 元平衡布尔函数至多是 $n-1$ 阶相关免疫的.

在定理 1 中,若取 $p=1/2$,则有

推论 2 设 $0<n_1<n$,$\forall\delta\in\{0,1\}^{n-n_1}$,$\varphi_\delta(x):\{0,1\}^{n_1}\to\{0,1\}$都是 $m(0\le m\le n_1-1)$阶相关免疫的平衡函数,则 $f(x,y)=\varphi_y(x)$ 也是 m 阶相关免疫的平衡函数.

设 $g(y)$ 是 $n-n_1$ 维布尔函数,因 $\forall\delta\in\{0,1\}^{n-n_1}$,由 $\varphi_\delta(x):\{0,1\}^{n_1}\to\{0,1\}$是 m 阶相关免疫的平衡函数可推出 $\varphi_\delta(x)\oplus g(\delta)$ 也是 m 阶相关免疫的平衡函数,故进一步有

推论 3[8] 设 $0<n_1<n$,$g(y)$ 是 $n-n_1$ 维布尔函数,若 $\forall\delta\in\{0,1\}^{n-n_1}$,$\varphi_\delta(x):\{0,1\}^{n_1}\to\{0,1\}$ 都是 $m(0\le m\le n_1-1)$阶相关免疫的平衡函数,则 $f(x,y)=\varphi_y(x)\oplus g(y)$ 也是 m 阶相关免疫的平衡函数.

注:在推论 3 中令 $\varphi_y(x)=\bigoplus_{j=1}^{n_1}x_j p_j(y)$ 即得文献[3]中的构造方法 2.

〈事实上,在构造方法 2 中,由于 $m=\min\{w(p_1(y),\cdots,p_{n_1}(y))\mid y\in\{0,1\}^{n-n_1}\}-1$,故 $\forall y\in\{0,1\}^{n-n_1}$,$\bigoplus_{j=1}^{n_1}x_j p_j(y)=p_1(y)x_1\oplus\cdots\oplus p_{n_1}(y)x_{n_1}$ 关于 x 都是一个至少有 $m+1$ 项系数不为 0 的线性函数,因而 $\forall y\in\{0,1\}^{n-n_1}$,$\bigoplus_{j=1}^{n_1}x_j p_j(y)$ 都是 m 阶相关免疫的平衡函数,由此可见,文献[3]中的构造方法 2 是推论 3 的特例〉.

由于文献[4]中的构造方法 3 与文献[3]中的构造方法 2 等价,故构造方法 3 也是推论 3 的特例.

引理 3[9] 设 Y 与 Z 均是二元随机变量,且其中之一是均匀分布,则 Y 与 Z 独立当且仅当 $Y\oplus Z$ 是平衡函数.

定理 2 设 $0<n_1<n$,若 $\forall\delta\in\{0,1\}^{n-n_1}$,$\varphi_\delta(x):\{0,1\}^{n_1}\to\{0,1\}$都是 $m(0\le m\le n_1-1)$阶相关免疫的平衡函数,且 $g(y)$ 是 $n-n_1$ 维的 $m'(0\le m'\le n-n_1-1)$阶相关免疫的平衡函数,则

$$f(x,y)=\varphi_y(x)\oplus g(y)$$

是 $m+m'+1$ 阶相关免疫的平衡函数.

证明 $\forall\delta\in\{0,1\}^{n-n_1}$,因 $\varphi_\delta(x)$ 是平衡函数,故 $f(x,\delta)=\varphi_\delta(x)\oplus g(\delta)$ 也是平衡函数,从而由推论 1 知 $f(x,y)=\varphi_y(x)\oplus g(y)$ 是平衡函数.

下证 $f(x,y)$ 是 $m+m'+1$ 阶相关免疫函数.

任取

$$1\le i_1<\cdots<i_r\le n_1,1\le j_1<\cdots<j_{m+m'+1-r}\le n-n_1\quad(r\le m+m'+1)$$

任意固定

$$x_{i_1}=a_1,\cdots,x_{i_r}=a_r;y_{j_1}=b_1,\cdots,y_{j_{m+m'+1-r}}=b_{m+m'+1-r}$$

分两种情况讨论:

(1) 设 $r\le m$,则对固定 δ,由 $\varphi_\delta(x)$ 是 m 阶相关免疫的平衡函数知,$\varphi_\delta(x)$ 必是 r 阶相关免疫的平衡函数,从而有

$$P[\varphi_\delta(x)=1|\ x_{i_1}=a_1,\cdots,x_{i_r}=a_r]=P[\varphi_\delta(x)=1]=1/2$$

于是,对满足 $y_{j_1}=b_1,\cdots,y_{j_{m+m'+1-r}}=b_{m+m'+1-r}$ 的给定 $y\in\{0,1\}^{n-n_1}$,有

$$P[\phi_y(x)=1\mid x_{i_1}=a_1,\cdots,x_{i_r}=a_r]=1/2$$

显然亦有

$$P[f(x,y)=\phi_y(x)\oplus g(y)=1\mid x_{i_1}=a_1,\cdots,x_{i_r}=a_r]=1/2$$

故由推论 1 知,在限定 $x_{i_1}=a_1,\cdots,x_{i_r}=a_r;y_{j_1}=b_1,\cdots,y_{j_{m+m'+1-r}}=b_{m+m'+1-r}$ 的条件下,有

$$P[f(x,y)=1]=1/2$$

即

$$P[f(x,y)=1\mid x_{i_1}=a_1,\cdots,x_{i_r}=a_r;y_{j_1}=b_1,\cdots,y_{j_{m+m'+1-r}}=b_{m+m'+1-r}]=1/2 \quad (1)$$

又 $f(x,y)=\phi_y(x)\oplus g(y)$ 是平衡函数,故有

$$P[f(x,y)=1]=1/2 \quad (2)$$

由式(1)、(2)知,$f(x,y)$ 是 $m+m'+1$ 阶相关免疫函数.

(2)设 $r>m$,则 $m+m'+1-r\le m'$,由 $g(y)$ 是 m' 阶相关免疫的平衡函数知,$g(y)$ 必是 $m+m'+1-r$ 阶相关免疫的平衡函数,从而有

$$P[g(y)=1\mid y_{j_1}=b_1,\cdots,y_{j_{m+m'+1-r}}=b_{m+m'+1-r}]=P[g(y)=1]=1/2$$

因 $g(y)$ 和 $f(x,y)=\phi_y(x)\oplus g(y)$ 均是平衡函数,故由引理 3 知,$\phi_y(x)$ 与 $g(y)$ 独立,于是有

$$\begin{aligned}
&P[f(x,y)=1\mid x_{i_1}=a_1,\cdots,x_{i_r}=a_r;\ y_{j_1}=b_1,\cdots,y_{j_{m+m'+1-r}}=b_{m+m'+1-r}]\\
&=P[\phi_y(x)\oplus g(y)=1\mid x_{i_1}=a_1,\cdots,x_{i_r}=a_r;\ y_{j_1}=b_1,\cdots,y_{j_{m+m'+1-r}}=b_{m+m'+1-r}]\\
&=P[\phi_y(x)=1,g(y)=0\mid x_{i_1}=a_1,\cdots,x_{i_r}=a_r;\ y_{j_1}=b_1,\cdots,y_{j_{m+m'+1-r}}=b_{m+m'+1-r}]\\
&+P[\phi_y(x)=0,g(y)=1\mid x_{i_1}=a_1,\cdots,x_{i_r}=a_r;\ y_{j_1}=b_1,\cdots,y_{j_{m+m'+1-r}}=b_{m+m'+1-r}]\\
&=P[\phi_y(x)=1\mid x_{i_1}=a_1,\cdots,x_{i_r}=a_r;\ y_{j_1}=b_1,\cdots,y_{j_{m+m'+1-r}}=b_{m+m'+1-r}]\\
&+P[g(y)=1\mid x_{i_1}=a_1,\cdots,x_{i_r}=a_r;\ y_{j_1}=b_1,\cdots,y_{j_{m+m'+1-r}}=b_{m+m'+1-r}]\\
&-2P[\phi_y(x)=1,g(y)=1\mid x_{i_1}=a_1,\cdots,x_{i_r}=a_r;\ y_{j_1}=b_1,\cdots,y_{j_{m+m'+1-r}}=b_{m+m'+1-r}]\\
&=P[\phi_y(x)=1\mid x_{i_1}=a_1,\cdots,x_{i_r}=a_r;\ y_{j_1}=b_1,\cdots,y_{j_{m+m'+1-r}}=b_{m+m'+1-r}]\\
&+P[g(y)=1\mid y_{j_1}=b_1,\cdots,y_{j_{m+m'+1-r}}=b_{m+m'+1-r}]\\
&-2P[\phi_y(x)=1\mid x_{i_1}=a_1,\cdots,x_{i_r}=a_r;\ y_{j_1}=b_1,\cdots,y_{j_{m+m'+1-r}}=b_{m+m'+1-r}]\\
&\cdot P[g(y)=1\mid y_{j_1}=b_1,\cdots,y_{j_{m+m'+1-r}}=b_{m+m'+1-r}]\\
&=1/2
\end{aligned}$$

故有

$$P[f(x,y)=1\mid x_{i_1}=a_1,\cdots,x_{i_r}=a_r;y_{j_1}=b_1,\cdots,y_{j_{m+m'+1-r}}=b_{m+m'+1-r}]=P[f(x,y)=1]$$

即 $f(x,y)$ 是 $m+m'+1$ 阶相关免疫函数.

注:在定理 2 中令 $\phi_y(x)=f_1(x)$,$g(y)=f_2(y)$,即得文献[2]中的结构定理 1;特别地,令 $\phi_y(x)=x_1\oplus 1$,$g(y)=f_2(y)$ 即得文献[6]中的结构定理 3.

推论 4　设 $g(x_m,\cdots,x_n)$ $(m<n)$ 是 1 阶相关免疫的平衡函数,则

$$f(x)=f(x_1,\cdots,x_n)=x_1\oplus\cdots\oplus x_{m-1}\oplus g(x_m,\cdots,x_n)$$

是 m 阶相关免疫的平衡函数.

4　m 阶相关免疫的平衡函数的计数

一般说来,平衡函数或近似平衡函数具有较高的密码学价值,因而我们在此仅讨论平衡的 m 阶相关免疫函数的计数.

记 $N^{(k)}(2^{l-1},l)$ 为 l 元 k 阶相关免疫的平衡函数的个数,则由推论 4 可得

引理 4[6]　$N^{(m)}(2^{n-1},n)\ge N^{(1)}(2^{n-m},n-m+1)$

定义 4[10]　称 $2k\times n$ 阶矩阵 C 为列平衡矩阵,当且仅当矩阵 C 各行互异,各列 0,1 各半.

显然,n 元布尔函数 $f(x)$ 是 1 阶相关免疫函数当且仅当其特征矩阵是列平衡矩阵.

引理 5　n 元 1 阶相关免疫的平衡函数的个数 $N^{(1)}(2^{n-1},n)$ 满足

$$N^{(1)}(2^{n-1},n)\ge C_{2^{n-1}}^{2^{n-2}}+\sum_{j=1}^{2^{n-3}}C_{2^{n-1}}^{2^j}\cdot C_{2^j}^{j}\cdot(C_{4j}^{2j})^{n-\lceil\log_2 j\rceil-3}\cdot C_{2^{n-1}-2^j}^{2^{n-2}-2^j}$$

其中 $\lceil x\rceil$ 表示不小于 x 的最小整数.

证明　(构造性证明. 通过构造 $2^{n-1}\times n$ 列平衡矩阵来构造 1 阶相关免疫的平衡函数. 构造思路是:使构造出来的 $2^{n-1}\times n$ 列平衡矩阵的行向量中两两互不共轭的有 $4j(j=0,1,\cdots,2^{n-3})$ 个,其余 $2^{n-1}-4j$ 个行向量以共轭对形式出现.)

(1)将 $\{0,1\}^n$ 中全部向量排成 2^{n-1} 个共轭对,从中任取 2^{n-2} 个共轭对组成的 $2^{n-1}\times n$ 矩阵一定是列平衡矩阵,按这种方法共可构造出 $C_{2^{n-1}}^{2^{n-2}}$ 个 $2^{n-1}\times n$ 列平衡矩阵.(相当于 $j=0$).

(2)首先,将 $\{0,1\}^{\lceil\log_2 4j\rceil}$ $(j=1,\cdots,2^{n-3})$ 即 $\{0,1\}^{\lceil\log_2 j\rceil+2}$ 中全部向量排成 $2^{\lceil\log_2 j\rceil+1}$ 个共轭对,从中任取 $2j$ 个共轭对组成 $4j\times(\lceil\log_2 j\rceil+2)$ 矩阵 A_1,按这种方法共可构造出 $C_{2^{\lceil\log_2 j\rceil+1}}^{2j}$ 个 $4j\times(\lceil\log_2 j\rceil+2)$ 矩阵;接着在矩阵 A_1 的第一列前添上一平衡列向量,要求每个共轭对前添上相同的 0 或 1,组成 $4j\times(\lceil\log_2 j\rceil+3)$ 矩阵 A_2,这种添法共有 C_{2j}^{j} 种;接着在矩阵 A_2 的第一列前依次添上 $n-\lceil\log_2 j\rceil-3$ 个平衡列向量组成 $4j\times n$ 矩阵 A_3,这种添法共有 $(C_{4j}^{2j})^{n-\lceil\log_2 j\rceil-3}$ 种;显然,矩阵 A_3 的行向

量互异且两两不共轭;最后,在矩阵 A_3 中添加 $2^{n-1}-4j$ 个两两共轭且不同于 A_3 中行向量的互异的 n 维行向量,组成 $2^{n-1}\times n$ 矩阵 A,这种添法共有 $C_{2^{n-1}-4j}^{2^{n-2}-2j}$ 种;显然,矩阵 A 是 $2^{n-1}\times n$ 列平衡矩阵,且按上述方法共可构造出 $\sum_{j=1}^{2^{n-3}} C_2^{2j}{}_{\lfloor\log_2 j\rfloor+1}\cdot C_{2j}^{j}\cdot(C_{4j}^{2j})^{n-\lfloor\log_2 j\rfloor-3}\cdot C_{2^{n-1}-4j}^{2^{n-2}-2j}$ 个 $2^{n-1}\times n$ 列平衡矩阵.

综合(1)、(2)可知,n 元 1 阶相关免疫的平衡函数至少有 $C_{2^{n-1}}^{2^{n-2}}+\sum_{j=1}^{2^{n-3}} C_2^{2j}{}_{\lfloor\log_2 j\rfloor+1}\cdot C_{2j}^{j}\cdot(C_{4j}^{2j})^{n-\lfloor\log_2 j\rfloor-3}\cdot C_{2^{n-1}-4j}^{2^{n-2}-2j}$ 个.

由引理 4、引理 5 即得

定理 3 n 元 m 阶相关免疫的平衡函数的个数 $N^{(m)}(2^{n-1},n)$ 满足

$$N^{(m)}(2^{n-1},n)\geq C_{2^{n-m}}^{2^{n-m-1}}+\sum_{j=1}^{2^{n-m-2}} C_2^{2j}{}_{\lfloor\log_2 j\rfloor+1}\cdot C_{2j}^{j}\cdot(C_{4j}^{2j})^{n-m-\lfloor\log_2 j\rfloor-2}\cdot C_{2^{n-m-1}-4j}^{2^{n-m-1}-2j}$$

容易推出,当定理 3 中的 j 取为 2 的方幂时,恰好就是文献[6]中 n 元 m 阶相关免疫的平衡函数的计数下界,这说明定理 3 给出的下界大大改进了已有的下界.

5 结束语

寻求相关免疫函数的简单构造方法并改进其计数下界具有重要意义.本文给出了两种构造相关免疫函数的新方法,并基于新方法改进了 m 阶相关免疫的平衡函数的计数下界.通过将新方法与几种已知的构造方法比较可知,几种已知的构造方法均是本文中构造方法的特殊情况,因此,本文的构造方法更具一般性.

参考文献:

[1] T Siegenthaler. Correlation immunity of nonlinear combining function for cryptographic applications[J]. IEEE Trans on IT, 1984, IT-30(5): 776 - 780.

[2] 杨义先,林须端,胡正名. 编码密码学[M]. 北京:人民邮电出版社,1992. 589 - 610.
Yang Yixian, Lin Xuduan, Hu Zhengming. Cryptography with Coding[M]. Beijing: People Posts and Telecommunications Press, 1992. 589 - 610. (in Chinese)

[3] P Camion, C Carlet, P Charpin, N Sendrier. On correlation-immune functions[A]. Advances in Cryptology-Crypto '91[C]. Berlin: Springer-Verlag, 1992. 86 - 100.

[4] J Seberry, X M Zhang, Y L Zheng. Construction and nonlinearity of correlation-immune functions[A]. Advances in Cryptology-Eurocrypt '93[C]. Berlin: Springer-Verlag, 1994. 181 - 199.

[5] 冯登国,肖国镇. 一类相关免疫函数的非线性性和扩散特性[J]. 通信学报,1996,17(2):70 - 74.
Feng Dengguo, Xiao Guozhen. Nonlinearity and propagation property of a family of correlation-immune functions[J]. Journal of China Institute of Communications, 1996, 17(2): 70 - 74. (in Chinese)

[6] 温巧燕,钮心忻,杨义先. 现代密码学中的布尔函数[M]. 北京:科学出版社,2000,66 - 83.
Wen Qiaoyan, Niu Xinxin, Yang Yixian. Boolean Functions in Modern Cryptography[M]. Beijing: Science Press, 2000. 66 - 83. (in Chinese)

[7] 冯登国,肖国镇. 对偶距离和相关免疫阶[J]. 通信学报,1994,15(1):15 - 16.
Feng Dengguo, Xiao Guozhen. The dual distance and correlation-immune order[J]. Journal of China Institute of Communications, 1994, 15(1): 15 - 16. (in Chinese)

[8] 郑浩然,金晨辉,张海模. 相关免疫置换的构造和计数[J]. 电子与信息学报,2003,25(5):711 - 715.
Zheng Haoran, Jin Chenhui, Zhang Haimo. Construction and enumeration of correlation-immune permutations[J]. Journal of Electronics & Information Technology, 2003, 25(5): 711 - 715. (in Chinese)

[9] 金晨辉. 多输出函数的平衡性判定[J]. 电子技术学院学报,1993,5(4):41 - 43.
Jin Chenhui. The balance judgment of multi-output functions[J]. Journal of Institute of Electronic Technology, 1993, 5(4): 41 - 43. (in Chinese)

[10] 杨义先. 相关免疫布尔函数的计数[J]. 电子科学学刊,1993,15(2):140 - 146.
Yang Yixian. Enumerating Boolean functions with correlation immunity[J]. Journal of Electronics, 1993, 15(2): 140 - 146. (in Chinese)

作者简介:

郑浩然 男,1968 年 3 月生于河南新蔡,解放军信息工程大学副教授.主要研究方向为密码学. E-mail: haoranzheng@126.com

金晨辉 男,1965 年 3 月生于河南扶沟,解放军信息工程大学 教授,博士生导师,主要研究方向为密码学和信息安全.