多输出布尔函数的相关免疫性

陈鲁生[1],徐汉良[2],符方伟[1]
(1. 南开大学数学科学学院,天津 300071;2. 中国科学技术大学研究生院信息安全国家重点实验室,北京 100039)

摘 要: 本文讨论多输出布尔函数的相关免疫性,证明了多输出相关免疫函数的一个性质,并给出了多输出相关免疫函数的一种构造方法.

关键词: 多输出布尔函数; 相关免疫函数; 无偏函数
中图分类号: TN918.1 **文献标识码**: A **文章编号**: 0372-2112 (2001) 04-0543-05

The Correlation Immunity of Multi-Output Boolean Functions

CHEN Lu-sheng[1], XU Han-liang[2], FU Fang-wei[1]
(1. *School of Mathematical Science, Nankai University, Tianjin* 300071, *China*;
2. *State Key Lab. of Information Security, Graduate School of USTC, Beijing* 100039, *China*)

Abstract: This paper discusses the correlation immunity of multi-output Boolean functions, shows a property of multi-output correlation immune functions and presents a method for constructing multi-output correlation immune functions.

Key words: multi-output Boolean function; correlation immune function; unbiased function

1 引言

布尔函数的相关免疫性首先在文献[1]中引入,它是衡量序列密码体制安全性的一个重要指标. 如果所选用的布尔函数不具有一定的相关免疫性,则相应的密码体制易受到相关分析法的攻击. 近年来,对单输出布尔函数的相关免疫性已进行了比较深入的研究,取得了许多重要成果. 但对多输出布尔函数的相关免疫性,目前比较深入的研究结果尚不多见. 文献[2]和[3]引入了多输出相关免疫函数的概念,并简略讨论了其密码学性质. 文献[4]对多输出布尔函数提出了一种相关分析方法.

本文讨论多输出布尔函数的相关免疫性,证明了多输出相关免疫函数的一个重要性质,并给出了多输出相关免疫函数的一种构造方法.

2 基本概念

设 $V_n = GF(2)^n$ 是二元域 $GF(2)$ 上的 n 维向量空间. 多输出布尔函数就是从 V_n 到 V_m 的函数. 对任意的从 V_n 到 V_m 的函数 F,它可以表示为 $F = (f_1, f_2, \cdots, f_m)$,其中每个分量函数 f_i 都是 V_n 上的函数,即 f_i 是从 V_n 到 $GF(2)$ 的函数,$1 \le i \le m$.

定义 1 设 F 是从 V_n 到 V_m 的函数. $X_1, X_2, \cdots, X_n$ 是二元域 $GF(2)$ 上的 n 个服从均匀分布并且相互独立的随机变量. 如果对任意 $\{j_1, j_2, \cdots, j_t\} \subseteq \{1, 2, \cdots, n\}$,随机变量 $Z = F(X_1, X_2, \cdots, X_n)$ 与 $(X_{j1}, X_{j2}, \cdots, X_{jt})$ 相互独立,即对任意 $(b_1, b_2, \cdots, b_t) \in V_t$ 和任意 $\alpha \in V_m$,

$$Pr(Z = \alpha \mid X_{ji} = b_i, 1 \le i \le t) = Pr(Z = \alpha),$$

则称 F 是 (n, m, t) 相关免疫函数.

定义 2 设 $n \ge m \ge 1$, F 是从 V_n 到 V_m 的函数. 如果对任意 $\alpha \in V_m$,

$$|\{x \in V_n \mid F(x) = \alpha\}| = 2^{n-m},$$

则称 F 是无偏函数. 对于 V_n 上的无偏函数,通常称之为平衡函数.

一般而言,无偏的相关免疫函数具有更好的密码学价值. 关于无偏函数的下述性质可在文献[5]中找到.

引理 1[5] $F = (f_1, f_2, \cdots, f_m)$ 是从 V_n 到 V_m 的无偏函数 $\Leftrightarrow F$ 的分量函数的每一个非零线性组合 $f(x) = \bigoplus_{i=1}^{m} c_i f_i(x)$ 都是 V_n 上的平衡函数,其中 $x \in V_n$, $c_1, c_2, \cdots, c_m \in GF(2)$ 并且不全为 0.

根据平衡函数的定义,下述结论是显然的.

引理 2 设 $f_i(y_i)$ 是 V_{n_i} 上的函数,其中 $y_i \in V_{n_i}$, $1 \le i \le r$. 如果 $f_i(y_i)$, $1 \le i \le r$ 中至少有一个是平衡函数,则

$$f(y_1, y_2, \cdots, y_r) = f_1(y_1) \oplus f_2(y_2) \oplus \cdots \oplus f_r(y_r)$$

也是平衡函数.

设 R 是实数域. 对任意从 V_n 到 R 的函数 g,

$$S_g(\omega) \stackrel{def}{=} \sum_{x \in V_n} g(x)(-1)^{<\omega, x>} \tag{1}$$

称为 g 的 Walsh 变换,其中 $\omega = (\omega_1, \omega_2, \cdots, \omega_n) \in V_n$, $x = (x_1, x_2, \cdots, x_n) \in V_n$,

收稿日期:1999-12-29;修回日期:2000-09-12
基金项目:国家自然科学基金(No. 69802008)

$$<\omega, x> = \bigoplus_{i=1}^{n}\omega_i x_i$$

是二元域上向量的内积. 容易验证, 对任意从 V_n 到 R 的函数 g 和任意的 $x \in V_n$,

$$g(x) = \frac{1}{2^n}\sum_{\omega\in V_n} S_g(\omega)(-1)^{<\omega, x>} \tag{2}$$

3 多输出相关免疫函数的一个性质

下面(定理 1)指出了多输出相关免疫函数的一个重要性质. 利用这个性质,可以将判断一个多输出布尔函数是否为 t 阶相关免疫函数转化为判断其每一个非零线性组合是否为 t 阶单输出相关免疫函数.

定理 1 $F = (f_1, f_2, \cdots, f_m)$ 是 (n, m, t) 相关免疫函数 $\Leftrightarrow F$ 的分量函数的每一个非零线性组合, $f(x) = \bigoplus_{i=1}^{m} c_i f_i(x)$ 都是 $(n, 1, t)$ 相关免疫函数,其中 $x \in V_n$, $c_1, c_2, \cdots, c_m \in GF(2)$ 并且不全为 0.

为了证明定理 1,先给出下面的两个引理.

引理 3 设 $\xi = (\xi_1, \xi_2, \cdots, \xi_m)$ 是 V_m 上的随机变量, $\alpha \in V_m$,则

$$Pr(\xi = \alpha) = \frac{1}{2^{m-1}}\sum_{\omega\in V_m} Pr(<\omega, \xi> = <\omega, \alpha>) - 1 \tag{3}$$

证明 显然,随机变量 ξ 的概率分布 $Pr(\xi = x)$ 是一个从 V_m 到 R 的函数,记 $g(x) = Pr(\xi = x)$, $x \in V_m$, 其 Walsh 变换为

$$S_g(\omega) = \sum_{x\in V_m}(-1)^{<\omega, x>} Pr(\xi = x) = Pr(<\omega, \xi> = 0)$$
$$- Pr(<\omega, \xi> = 1) = 2\,Pr(<\omega, \xi> = 0) - 1$$

根据式(2),有

$$Pr(\xi = \alpha) = \frac{1}{2^m}\sum_{\omega\in V_m}(-1)^{<\omega, \alpha>} S_g(\omega)$$
$$= \frac{1}{2^m}\sum_{\omega\in V_m}(-1)^{<\omega, \alpha>}(2\,Pr(<\omega, \xi> = 0) - 1)$$
$$= \frac{1}{2^{m-1}}\sum_{\omega\in V_m}(-1)^{<\omega, \alpha>} Pr(<\omega, \xi> = 0)$$
$$- \frac{1}{2^m}\sum_{\omega\in V_m}(-1)^{<\omega, \alpha>}$$

当 α 为 V_m 中的零向量时,显然,

$$Pr(\xi = 0) = \frac{1}{2^{m-1}}\sum_{\omega\in V_m} Pr(<\omega, \xi> = 0) - 1$$

当 α 不为 V_m 中的零向量时, 由于 $\sum_{\omega\in V_m}(-1)^{<\omega, \alpha>} = 0$ 以及

$$(-1)^{<\omega, \alpha>} Pr(<\omega, \xi> = 0)$$
$$= Pr(<\omega, \xi> = <\omega, \alpha>) - <\omega, \alpha>$$

故

$$Pr(\xi = \alpha) = \frac{1}{2^{m-1}}\sum_{\omega\in V_m}(Pr(<\omega, \xi> = <\omega, \alpha>) - <\omega, \alpha>)$$
$$= \frac{1}{2^{m-1}}\sum_{\omega\in V_m} Pr(<\omega, \xi> = <\omega, \alpha>) - \frac{1}{2^{m-1}}\sum_{\omega\in V_n} <\omega, \alpha>$$
$$= \frac{1}{2^{m-1}}\sum_{\omega\in V_m} Pr(<\omega, \xi> = <\omega, \alpha>) - 1$$

因此,对任意 $\alpha \in V_m$,式(3)成立. □

引理 4 设 $\eta = (\eta_1, \eta_2, \cdots, \eta_t)$ 是 V_t 上的随机变量, $\xi = (\xi_1, \xi_2, \cdots, \xi_m)$ 是 V_m 上的随机变量,则 η 与 $\xi = (\xi_1, \xi_2, \cdots, \xi_m)$ 相互独立 $\Leftrightarrow \eta$ 与 $\xi_1, \xi_2, \cdots, \xi_n$ 的每一个非零线性组合 $\bigoplus_{i=1}^{m} c_i\xi_i$ 相互独立,其中 $c_1, c_2, \cdots, c_m \in GF(2)$ 并且不全为 0.

证明 对任意 $c_1, c_2, \cdots, c_m \in GF(2)$ 并且不全为 0, $c \in GF(2)$,令

$$T_c(c_1, c_2, \cdots, c_m) = \{\alpha \mid \alpha = (a_1, a_2, \cdots, a_m) \in V_m, \bigoplus_{i=1}^{m} c_i a_i = c\}$$

假设 η 与 $\xi = (\xi_1, \xi_2, \cdots, \xi_m)$ 相互独立,则对任意 $\beta \in V_t$,

$$Pr(\bigoplus_{i=1}^{m} c_i\xi_i = c \mid \eta = \beta) = \sum_{\alpha\in T_c(c_1, c_2, \cdots, c_m)} Pr(\xi = \alpha \mid \eta = \beta)$$
$$= \sum_{\alpha\in T_c(c_1, c_2, \cdots, c_m)} Pr(\xi = \alpha)$$
$$= Pr(\bigoplus_{i=1}^{m} c_i\xi_i = c)$$

因此, η 与 $\xi_1, \xi_2, \cdots, \xi_m$ 的每一个非零线性组合 $\bigoplus_{i=1}^{m} c_i\xi_i$ 相互独立.

反过来,假设 η 与 $\xi_1, \xi_2, \cdots, \xi_m$ 的每一个非零线性组合 $\bigoplus_{i=1}^{m} c_i\xi_i$ 相互独立,则对任意 $\omega, \alpha \in V_m$ 以及 $\beta \in V_t$,

$$Pr(<\omega, \xi> = <\omega, \alpha> \mid \eta = \beta) = Pr(<\omega, \xi> = <\omega, \alpha>)$$

根据引理 3,有

$$Pr(\xi = \alpha \mid \eta = \beta) = \frac{1}{2^{m-1}}\sum_{\omega\in V_m} Pr(<\omega, \xi> = <\omega, \alpha> \mid \eta = \beta) - 1$$
$$= \frac{1}{2^{m-1}}\sum_{\omega\in V_m} Pr(<\omega, \xi> = <\omega, \alpha>) - 1$$
$$= Pr(\xi = \alpha).$$

因此, η 与 $\xi = (\xi_1, \xi_2, \cdots, \xi_m)$ 相互独立. □

证明(定理 1) 设 $X_1, X_2, \cdots, X_n$ 是二元域 $GF(2)$ 上的 n 个服从均匀分布并且相互独立的随机变量, $Z_i = f_i(X_1, X_2, \cdots, X_n)$, $i = 1, 2, \cdots, m$. 根据定义 1 和引理 4, $F = (f_1, f_2, \cdots, f_m)$ 是 (n, m, t) 相关免疫函数 $\Leftrightarrow$ 对任意 $\{j_1, j_2, \cdots, j_t\} \subseteq \{1, 2, \cdots, n\}$,随机变量

$$Z = F(X_1, X_2, \cdots, X_n) = (Z_1, Z_2, \cdots, Z_m)$$

与 $(X_{j1}, X_{j2}, \cdots, X_{jt})$ 相互独立 $\Leftrightarrow$ 对任意 $\{j_1, j_2, \cdots, j_t\} \subseteq \{1, 2, \cdots, n\}$, $Z_1, Z_2, \cdots, Z_m$ 的每一个非零线性组合

$$\bigoplus_{i=1}^{m} c_i Z_i = \bigoplus_{i=1}^{m} c_i f_i(X_1, X_2, \cdots, X_n)$$

与 $(X_{j1}, X_{j2}, \cdots, X_{jt})$ 相互独立 $\Leftrightarrow F$ 的分量函数的每一个非零线性组合 $\bigoplus_{i=1}^{m} c_i f_i(x)$ 都是 $(n, 1, t)$ 相关免疫函数,其中 $x \in V_n$.

4 多输出相关免疫函数的构造

引理 5[6] 设 $f_1(y_1)$ 是 $(n_1, 1, t_1)$ 相关免疫函数, $f_2(y_2)$ 是 $(n_2, 1, t_2)$ 相关免疫函数, $t_1 \le t_2$, $y_1 \in V_{n1}$, $y_2 \in V_{n2}$. 设

$$f(y_1, y_2) = f_1(y_1) \oplus f_2(y_2).$$

(1)若 f_1 和 f_2 都不是平衡函数,则 f 是 $(n_1 + n_2, 1, t_1)$ 相关免疫函数.

(2)若 f_1 不是平衡函数, f_2 是平衡函数,则 f 是 $(n_1 + n_2, 1, t_2)$ 相关免疫函数.

(3)若 f_1 是平衡函数, f_2 不是平衡函数,则 f 是 $(n_1 + n_2,$

$1, t_1)$相关免疫函数.

(4)若 f_1 和 f_2 都是平衡函数,则 f 是$(n_1+n_2, 1, t_1+t_2+1)$相关免疫函数.

为了将上述引理推广到多个单输出相关免疫函数的加和的情形,先引进一个相关免疫函数的阶函数.

设 $N=\{0,1,2,3,\cdots\}$是所有非负整数的集合. ψ是一个从 $\cup_{n=1}^{\infty}(\{0,1\}^n\times N^n)$到 N 的函数,ψ由以下递推关系定义.

(1)对任意 $n\geq 2$,$(b_1,b_2,\cdots,b_n)\in\{0,1\}^n$ 和$(t_1,t_2,\cdots,t_n)\in N^n$,$\psi((b_1,b_2,\cdots,b_n),(t_1,t_2,\cdots,t_n))=\psi((b_{j1},b_{j2},\cdots,b_{jn}),(t_{j1},t_{j2},\cdots,t_{jn}))$,其中$\{j_1,j_2,\cdots,j_n\}$是满足 $t_{j1}\leq t_{j2}\leq\cdots\leq t_{jn}$的$\{1,2,\cdots,n\}$的一个排列.

(2)对任意 $n>2$,$(b_1,b_2,\cdots,b_n)\in\{0,1\}^n$)和$(t_1,t_2,\cdots,t_n)\in N^n$,若 $t_1\leq t_2\leq\cdots\leq t_n$,则

当$(b_1,\cdots,b_{\lfloor n/2\rfloor})$和$(b_{\lfloor n/2\rfloor+1},\cdots,b_n)$都是零向量时,$\psi((b_1,b_2,\cdots,b_n),(t_1,t_2,\cdots,t_n))=\psi((b_1,\cdots,b_{\lfloor n/2\rfloor}),(t_1,\cdots,t_{\lfloor n/2\rfloor}))$.

当$(b_1,\cdots,b_{\lfloor n/2\rfloor})$是零向量,$(b_{\lfloor n/2\rfloor+1},\cdots,b_n)$不是零向量时,

$\psi((b_1,b_2,\cdots,b_n),(t_1,t_2,\cdots,t_n))=\psi((b_{\lfloor n/2\rfloor+1},\cdots,b_n),(t_{\lfloor n/2\rfloor+1},\cdots,t_n))$.

当$(b_1,\cdots,b_{\lfloor n/2\rfloor})$不是零向量,$(b_{\lfloor n/2\rfloor+1},\cdots,b_n)$是零向量时,$\psi((b_1,b_2,\cdots,b_n),(t_1,t_2,\cdots,t_n))=\psi((b_1,\cdots,b_{\lfloor n/2\rfloor}),(t_1,\cdots,t_{\lfloor n/2\rfloor}))$.

当$(b_1,\cdots,b_{\lfloor n/2\rfloor})$和$(b_{\lfloor n/2\rfloor+1},\cdots,b_n)$都不是零向量时,

$\psi((b_1,b_2,\cdots,b_n),(t_1,t_2,\cdots,t_n))=\psi((b_1,\cdots,b_{\lfloor n/2\rfloor}),(t_1,\cdots,t_{\lfloor n/2\rfloor}))+\psi((b_{\lfloor n/2\rfloor+1},\cdots,b_n),(t_{\lfloor n/2\rfloor+1},\cdots,t_n))+1$

这里$\lfloor n/2\rfloor$表示不大于 $n/2$ 的最大整数.

(3)对任意$(b_1,b_2)\in\{0,1\}^2$和$(t_1,t_2)\in N^2$,若 $t_1\leq t_2$,则

$$\psi((b_1,b_2),(t_1,t_2))=\begin{cases}t_1, & \text{如果 } b_1=0,\ b_2=0;\\ t_2, & \text{如果 } b_1=0,\ b_2=1;\\ t_1, & \text{如果 } b_1=1,\ b_2=0;\\ t_1+t_2+1, & \text{如果 } b_1=1,\ b_2=1.\end{cases}$$

(4)对任意 $b_1\in\{0,1\}$和 $t_1\in N$,$\psi(b_1,t_1)=t_1$.

例　设 $t_1\leq t_2\leq t_3\leq t_4$,则

$$\psi((0,1,1,0),(t_1,t_2,t_3,t_4))=\psi((0,1),(t_1,t_2))+\psi((1,0),(t_3,t_4))+1=t_2+t_3+1.$$

下面的引理 6 是引理 5 的一个推广.

引理 6　设 $f_i(y_i)$是$(n_i,1,t_i)$相关免疫函数,其中 $y_i\in V_{n_i}, 1\leq i\leq r$. 则

$$f(y_1,y_2,\cdots,y_r)=f_1(y_1)\oplus f_2(y_2)\oplus\cdots\oplus f_r(y_r)$$

是$(\sum_{i=1}^{r}n_i,1,t)$相关免疫函数,其中 $t=\psi((b_1,b_2,\cdots,b_r),(t_1,t_2,\cdots,t_r))$,

$$b_i=\begin{cases}1, & \text{如果 } f_i(y_i)\text{是平衡函数},\\ 0, & \text{如果 } f_i(y_i)\text{不是平衡函数},\end{cases}\quad i=1,2,\cdots,r.$$

证明　因为对$\{1,2,\cdots,r\}$的任意一个排列$\{j_1,j_2,\cdots,j_r\}$,

$$f_{j_1}(y_{j_1})\oplus f_{j_2}(y_{j_2})\oplus\cdots\oplus f_{j_r}(y_{j_r})=f_1(y_1)\oplus f_2(y_2)\oplus\cdots\oplus f_r(y_r)=f(y_1,y_2,\cdots,y_r),$$

所以不妨假设 $t_1\leq t_2\leq\cdots\leq t_r$.

下面用归纳法证明本引理的结论成立.

当 $r=2$ 时,由引理 5 和相关免疫函数的阶函数 ψ的定义可知结论成立.

假设当 $r<k$ 时, 结论成立.

当 $r=k$ 时,设

$g_1(y_1,\cdots,y_{\lfloor k/2\rfloor})=f_1(y_1)\oplus\cdots\oplus f_{\lfloor k/2\rfloor}(y_{\lfloor k/2\rfloor})$,

$g_2(y_{\lfloor k/2\rfloor+1},\cdots,y_k)=f_{\lfloor k/2\rfloor+1}(y_{\lfloor k/2\rfloor+1})\oplus\cdots\oplus f_k(y_k)$,则

$f(y_1,y_2,\cdots,y_k)=g_1(y_1,\cdots,y_{\lfloor k/2\rfloor})\oplus g_2(y_{\lfloor k/2\rfloor+1},\cdots,y_k)$.

由归纳假设知,$g_1(y_1,\cdots,y_{\lfloor k/2\rfloor})$是$(\sum_{i=1}^{\lfloor k/2\rfloor}n_i,1,s_1)$相关免疫函数,其中

$$s_1=\psi((b_1,\cdots,b_{\lfloor k/2\rfloor}),(t_1,\cdots,t_{\lfloor k/2\rfloor})).$$

$g_2(y_{\lfloor k/2\rfloor+1},\cdots,y_k)$是$(\sum_{i=\lfloor k/2\rfloor+1}^{k}n_i,1,s_2)$相关免疫函数,其中

$$s_2=\psi((b_{\lfloor k/2\rfloor+1},\cdots,b_k),(t_{\lfloor k/2\rfloor+1},\cdots,t_k)).$$

因为 $t_1\leq t_2\leq\cdots\leq t_n$,所以 $\sum_{i=1}^{\lfloor k/2\rfloor}t_i\leq\sum_{i=\lfloor k/2\rfloor+1}^{k}t_i$. 由引理 2 知,当$(b_1,\cdots,b_{\lfloor k/2\rfloor})$不是零向量时,$g_1(y_1,\cdots,y_{\lfloor k/2\rfloor})$是平衡函数,当$(b_{\lfloor k/2\rfloor+1},\cdots,b_k)$不是零向量时,$g_2(y_{\lfloor k/2\rfloor+1},\cdots,y_k)$是平衡函数. 因此, 根据引理 5 和相关免疫函数的阶函数 ψ的定义可知,$f(y_1,y_2,\cdots,y_k)$是$(\sum_{i=1}^{k}n_i,1,t)$相关免疫函数,其中 $t=\psi((b_1,b_2,\cdots,b_k),(t_1,t_2,\cdots,t_k))$. □

定理 2　设 $F_j=(f_{j1},f_{j2},\cdots,f_{jm})$是$(n_j,m,t_j)$相关免疫函数,$j=1,2,\cdots,r$. 设 $A=(a_{ij})_{r\times s}$是 $GF(2)$ 上的 $r\times s$ 阶矩阵,$r\geq s$,$\mathrm{Rank}(A)=s$,ρ为由 A^T 生成的线性码的极小重量. 设

$$F(y_1,y_2,\cdots,y_r)=(F_1(y_1),F_2(y_2),\cdots,F_r(y_r))A,$$

其中 $y_j\in V_{n_j}$, $j=1,2,\cdots,r$. 则 $F(y_1,y_2,\cdots,y_r)$是$(\sum_{i=1}^{r}n_j,sm,t)$相关免疫函数,其中

$$t=\min_{1\leq j_1<j_2<\cdots<j_\rho\leq r}\psi((b_{j_1},b_{j_2},\cdots,b_{j_\rho}),(t_{j_1},t_{j_2},\cdots,t_{j_\rho})),\quad (4)$$

$$b_j=\begin{cases}1, & \text{如果 } F_j\text{ 是无偏函数},\\ 0, & \text{如果 } F_j\text{ 不是无偏函数}.\end{cases}\quad j=1,2,\cdots,r.$$

进一步,若 $F_1,F_2,\cdots,F_r$ 中至少有 $r-\rho+1$ 个是无偏函数,则 $F(y_1,y_2,\cdots,y_r)$是无偏的$(\sum_{i=1}^{r}n_j,sm,t)$相关免疫函数,其中 t 由式(4)定义.

证明　对任意的 $k,1\leq k\leq s$,

$$(F_1(y_1),F_2(y_2),\cdots,F_r(y_r))\begin{pmatrix}a_{1k}\\ a_{2k}\\ \cdots\\ a_{rk}\end{pmatrix}=a_{1k}F_1(y_1)\oplus a_{2k}F_2(y_2)\oplus\cdots\oplus a_{rk}F_r(y_r)=(\bigoplus_{j=1}^{r}a_{jk}f_{j1}(y_j),\bigoplus_{j=1}^{r}a_{jk}f_{j2}(y_j),\cdots,\bigoplus_{j=1}^{r}a_{jk}f_{jm}(y_j)).$$

考虑 F 的分量函数的任意非零线性组合,

$$\begin{aligned}f(y_1,y_2,\cdots,y_r)=&c_{11}\bigoplus_{j=1}^{r}a_{j1}f_{j1}(y_j)\oplus c_{12}\bigoplus_{j=1}^{r}a_{j1}f_{j2}(y_j)\oplus\cdots\oplus c_{1m}\\ &\bigoplus_{j=1}^{r}a_{j1}f_{jm}(y_j)\oplus c_{21}\bigoplus_{j=1}^{r}a_{j2}f_{j1}(y_j)\oplus c_{22}\bigoplus_{j=1}^{r}a_{j2}f_{j2}(y_j)\\ &\oplus\cdots\oplus c_{2m}\bigoplus_{j=1}^{r}a_{j2}f_{jm}(y_j)\oplus\cdots\cdots\\ &\oplus c_{s1}\bigoplus_{j=1}^{r}a_{js}f_{j1}(y_j)\oplus c_{s2}\bigoplus_{j=1}^{r}a_{js}f_{j2}(y_j)\oplus\cdots\oplus c_{sm}\end{aligned}$$

$$\bigoplus_{j=1}^{r} a_{js} f_{jm}(y_j) = \bigoplus_{k=1}^{s}\bigoplus_{i=1}^{m} c_{ki}\bigoplus_{j=1}^{r} a_{jk} f_{ji}(y_j) = \bigoplus_{j=1}^{r}\bigoplus_{k=1}^{s} a_{jk}$$

$$\bigoplus_{i=1}^{m} c_{ki} f_{ji}(y_j) = a_{11}\bigoplus_{i=1}^{m} c_{1i} f_{1i}(y_1) \oplus a_{12}\bigoplus_{i=1}^{m} c_{2i} f_{1i}(y_1)$$

$$\oplus\cdots\oplus a_{1s}\bigoplus_{i=1}^{m} c_{si} f_{1i}(y_1) \oplus a_{21}\bigoplus_{i=1}^{m} c_{1i} f_{2i}(y_2) \oplus a_{22}$$

$$\bigoplus_{i=1}^{m} c_{2i} f_{2i}(y_2) \oplus\cdots\oplus a_{2s}\bigoplus_{i=1}^{m} c_{si} f_{2i}(y_2) \oplus\cdots\cdots$$

$$\oplus a_{r1}\bigoplus_{i=1}^{m} c_{1i} f_{ri}(y_r) \oplus a_{r2}\bigoplus_{i=1}^{m} c_{2i} f_{ri}(y_r) \oplus\cdots\oplus a_{rs}$$

$$\bigoplus_{i=1}^{m} c_{si} f_{ri}(y_r).$$

令

$$C = \begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1m} \\ c_{21} & c_{22} & \cdots & c_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ c_{s1} & c_{s2} & \cdots & c_{sm} \end{pmatrix}_{s\times m}, \quad \boldsymbol{\beta}_i = \begin{pmatrix} c_{1i} \\ c_{2i} \\ \cdots \\ c_{si} \end{pmatrix}, \ i = 1, 2, \cdots, m.$$

$\boldsymbol{\alpha}_j = (a_{j1}, a_{j2}, \cdots, a_{js})$, $j = 1, 2, \cdots, r$.

则

$$f(y_1, y_2, \cdots, y_r) = \bigoplus_{i=1}^{m} \boldsymbol{\alpha}_1\boldsymbol{\beta}_i f_{1i}(y_1) \oplus \bigoplus_{i=1}^{m} \boldsymbol{\alpha}_2\boldsymbol{\beta}_i f_{2i}(y_2) \oplus\cdots$$

$$\oplus\bigoplus_{i=1}^{m} \boldsymbol{\alpha}_r\boldsymbol{\beta}_i f_{ri}(y_r)$$

设 $A_{r\times s}C_{s\times m} = B_{r\times m}$，则 B 的每一列都是 A 的列向量的线性组合. 由于 C 是任意的非零布尔矩阵，所以当 C 的第 j 列不全为零时，B 的第 j 列中至少有 ρ 个 1，ρ 是由 A^T 生成的线性码的极小重量. 当 C 的第 j 列全为零时，B 的第 j 列也全为零. 因此，B 中至少有 ρ 行不为零向量. 事实上，若 B 中仅有 μ 行不为零向量，$\mu < \rho$，则 B 中每一列上 1 的个数 $\leq \mu < \rho$. 但是，因为 C 是任意的非零布尔矩阵，所以 B 中至少有一列，其上 1 的个数 $\geq \rho$，矛盾.

因为

$$AC = B = \begin{pmatrix} \boldsymbol{\alpha}_1\boldsymbol{\beta}_1 & \boldsymbol{\alpha}_1\boldsymbol{\beta}_2 & \cdots & \boldsymbol{\alpha}_1\boldsymbol{\beta}_m \\ \boldsymbol{\alpha}_2\boldsymbol{\beta}_1 & \boldsymbol{\alpha}_2\boldsymbol{\beta}_2 & \cdots & \boldsymbol{\alpha}_2\boldsymbol{\beta}_m \\ \cdots & \cdots & \cdots & \cdots \\ \boldsymbol{\alpha}_r\boldsymbol{\beta}_1 & \boldsymbol{\alpha}_r\boldsymbol{\beta}_2 & \cdots & \boldsymbol{\alpha}_r\boldsymbol{\beta}_m \end{pmatrix},$$

所以，$(\boldsymbol{\alpha}_j\boldsymbol{\beta}_1, \boldsymbol{\alpha}_j\boldsymbol{\beta}_2, \cdots, \boldsymbol{\alpha}_j\boldsymbol{\beta}_m)$，$j = 1, 2, \cdots, r$ 中至少有 ρ 个不为零向量. 于是

$$\bigoplus_{i=1}^{m} \boldsymbol{\alpha}_1\boldsymbol{\beta}_i f_{1i}(y_1), \bigoplus_{i=1}^{m} \boldsymbol{\alpha}_2\boldsymbol{\beta}_i f_{2i}(y_2), \cdots, \bigoplus_{i=1}^{m} \boldsymbol{\alpha}_r\boldsymbol{\beta}_i f_{ri}(y_r)$$

中至少有 ρ 个不为零.

因为 $F_j(y_j) = (f_{j1}(y_j), f_{j2}(y_j), \cdots, f_{jm}(y_j))$ 是 (n_j, m, t_j) 相关免疫函数，所以由定理 1 知，当 $(\boldsymbol{\alpha}_j\boldsymbol{\beta}_1, \boldsymbol{\alpha}_j\boldsymbol{\beta}_2, \cdots, \boldsymbol{\alpha}_j\boldsymbol{\beta}_m)$ 不为零向量时，$\bigoplus_{i=1}^{m} \boldsymbol{\alpha}_j\boldsymbol{\beta}_i f_{ji}(y_j)$ 是 $(n_j, 1, t_j)$ 相关免疫函数，$j = 1, 2, \cdots, r$.

根据引理 6 知，$f(y_1, y_2, \cdots, y_r)$ 是 $(\sum_{j=1}^{r} n_j, 1, t)$ 相关免疫函数，其中 t 由式(4)定义. 再由定理 1 知 $F(y_1, y_2, \cdots, y_r)$ 是 $(\sum_{j=1}^{r} n_j, sm, t)$ 相关免疫函数.

进一步，如果 $F_1, F_2, \cdots, F_r$ 中至少有 $r - \rho + 1$ 个是无偏函数，则由引理 1 知，

$$\bigoplus_{i=1}^{m} \boldsymbol{\alpha}_1\boldsymbol{\beta}_i f_{1i}(y_1), \bigoplus_{i=1}^{m} \boldsymbol{\alpha}_2\boldsymbol{\beta}_i f_{2i}(y_2), \cdots, \bigoplus_{i=1}^{m} \boldsymbol{\alpha}_r\boldsymbol{\beta}_i f_{ri}(y_r)$$

中至少有一个是平衡函数. 因此，由引理 2 知，$f(y_1, y_2, \cdots, y_r)$ 是平衡函数. 再由引理 1 知，$F(y_1, y_2, \cdots, y_r)$ 是从 V_n 到 V_{sm} 的无偏函数，其中 $n = \sum_{j=1}^{r} n_j$. □

推论 1 设 $F = (f_1, f_2, \cdots, f_m)$ 是 (n, m, t) 相关免疫函数，$A = (a_{ij})_{r\times s}$ 是 $GF(2)$ 上的 $r\times s$ 阶矩阵，$r \geq s$，$\mathrm{Rank}(A) = s$，ρ 为由 A^T 生成的线性码的极小重量. 设

$$G(y_1, y_2, \cdots, y_r) = (F(y_1), F(y_2), \cdots, F(y_r))A,$$

其中 $y_j \in V_n$，$j = 1, 2, \cdots, r$. 若 F 不是无偏函数，则 $G(y_1, y_2, \cdots, y_r)$ 是 (rn, sm, t) 相关免疫函数. 若 F 是无偏函数，则 $G(y_1, y_2, \cdots, y_r)$ 是无偏的 $(rn, sm, \rho t + \rho - 1)$ 相关免疫函数.

证明 由定理 2 知，$G(y_1, y_2, \cdots, y_r)$ 是 (rn, sm, q) 相关免疫函数，并且当 F 是无偏函数时，$G(y_1, y_2, \cdots, y_r)$ 是无偏的 (rn, sm, q) 相关免疫函数，其中

$$q = \psi(\underbrace{(b, b, \cdots, b)}_{\rho}, \underbrace{(t, t, \cdots, t)}_{\rho}),$$

$$b = \begin{cases} 1, & \text{如果 } F \text{ 是无偏函数}, \\ 0, & \text{如果 } F \text{ 不是无偏函数}. \end{cases}$$

根据相关免疫函数的阶函数 ψ 的定义，当 $b = 0$ 时，容易计算

$$q = \psi(\underbrace{(0, 0, \cdots, 0)}_{\rho}, \underbrace{(t, t, \cdots, t)}_{\rho}) = t,$$

当 $b = 1$ 时，容易计算

$$q = \psi(\underbrace{(1, 1, \cdots, 1)}_{\rho}, \underbrace{(t, t, \cdots, t)}_{\rho}) = \rho t + \rho - 1. \qquad \square$$

推论 2 设 $F_j = (f_{j1}, f_{j2}, \cdots, f_{jm})$ 是无偏的 (n_j, m, t_j) 相关免疫函数，$j = 1, 2, \cdots, r$. 设 $A = (a_{ij})_{r\times s}$ 是 $GF(2)$ 上的 $r\times s$ 阶矩阵，$r \geq s$，$\mathrm{Rank}(A) = s$，ρ 为由 A^T 生成的线性码的极小重量. 设

$$\tau = \sum_{k=1}^{\rho} t_{i_k}$$

其中 $\{i_1, i_2, \cdots, i_r\}$ 是满足 $t_{i_1} \leq t_{i_2} \leq \cdots \leq t_{i_r}$ 的 $\{1, 2, \cdots, r\}$ 的一个排列. 则

$$F(y_1, y_2, \cdots, y_r) = (F_1(y_1), F_2(y_2), \cdots, F_r(y_r))A$$

是无偏的 $(\sum_{j=1}^{r} n_j, sm, \tau + \rho - 1)$ 相关免疫函数，其中 $y_j \in V_{n_j}$，$j = 1, 2, \cdots, r$.

证明 因为 F_j 是无偏的 (n_j, m, t_j) 相关免疫函数，$j = 1, 2, \cdots, r$，所以根据定理 2 知，$F(y_1, y_2, \cdots, y_r)$ 是无偏的 $(\sum_{j=1}^{r} n_j, sm, t)$ 相关免疫函数，其中

$$t = \min_{1\leq j_1 < j_2 < \cdots < j_\rho \leq r} \psi(\underbrace{(1, 1, \cdots, 1)}_{\rho}, (t_{j_1}, t_{j_2}, \cdots, t_{j_\rho}))$$

根据 ψ 的定义，容易计算

$$\psi(\underbrace{(1, 1, \cdots, 1)}_{\rho}, (t_{j_1}, t_{j_2}, \cdots, t_{j_\rho})) = \sum_{k=1}^{\rho} t_{j_k} + \rho - 1$$

因此，

$$t = \min_{1\leq j_1 < j_2 < \cdots < j_\rho \leq r} (\sum_{k=1}^{\rho} t_{j_k} + \rho - 1) = \sum_{k=1}^{\rho} t_{i_k} + \rho - 1$$

其中 $\{i_1, i_2, \cdots, i_r\}$ 是满足 $t_{i_1} \leq t_{i_2} \leq \cdots \leq t_{i_r}$ 的 $\{1, 2, \cdots, r\}$ 的一个排列. □

5 结束语

文献[3]指出定理 1 的逆命题不成立并给出了一个反例. 经过仔细验证，发现文献[3]中的反例实际上是支持定理 1 的

逆命题的.从定理 1 可以看出,多输出相关免疫函数可以抵抗对其分量函数的任意非零线性组合进行的相关分析攻击.定理 2 给出了多输出相关免疫函数的一种构造方法.它是引理 5 给出的单输出相关免疫函数构造方法的一个显著推广.另外,推论 2 就是文献[7]中的定理 1 给出的结果.因此,定理 2 也可以看做是文献[7]中定理 1 的一个推广.实际上,定理 2 的证明方法就是借鉴了文献[7]中定理 1 的证明技巧.

参考文献:

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

[2] K. Gopalakrishnan and D. R. Stinson. Three characterizations of non-binary correlation immune and resilient functions [J]. Designs, Codes and Cryptography, 1995, 5: 241 - 251.

[3] 丁存生,肖国镇.流密码学及其应用 [M].北京:国防工业出版社,1994: 169 - 173.

[4] 胡一平, 冯登国.多输出前馈函数的一种相关分析方法 [J].电子科学学刊,1998, 20(6): 787 - 793.

[5] X. M. Zhang and Y. Zheng. Cryptographically resilient functions [J]. IEEE Trans. Inform. Theory, 1997, 43(5): 1740 - 1747.

[6] 杨义先,林须端.编码密码学 [M].北京:人民邮电出版社, 1992: 600 - 604.

[7] L. S. Chen and F. W. Fu. On the constructions of new resilient functions from old ones [J]. IEEE Trans. Inform. Theory, 1999, 45(6): 2077 - 2082.

作者简介:

陈鲁生　1962 年 10 月生,博士,南开大学数学科学学院副教授.目前主要研究方向为密码学理论,形式语言和自动机理论等.

徐汉良　1964 年 2 月生,博士,1985 年毕业于郑州信息工程大学应用数学系,副研究员,现在中国科技大学研究生院作博士后.主要研究方向为密码学理论及其应用等.

符方伟　1963 年 10 月生,南开大学数学科学学院教授,博士生导师.主要研究方向为信息论,编码理论,密码学理论和数字通信原理等.