# 多输出相关免疫逻辑函数的等价刻划及其应用[1]

徐汉良 吕述望

(中国科学院研究生院信息安全国家重点实验室 北京 100039)

**摘 要** 该文对多输出逻辑函数相关免疫性的两种刻划进行了讨论，在利用 Walsh 变换理论导出二元随机向量概率分布分解式的基础上，证明了两种刻划的等价性，并利用多输出相关免疫逻辑函数构造了一类不具有输入输出线性组合符合优势的密钥流生成器。

**关键词** 多输出逻辑函数，相关免疫性，Walsh 变换，等价定理，密钥流生成器

**中图号** TN918.1

## 1 引 言

若对 $F_2^n$ 中的每个向量 $\boldsymbol{X}=(x_1,x_2,\cdots,x_n)$ 都有 $F_2^m$ 中唯一的向量 $\boldsymbol{Y}=(y_1,y_2,\cdots,y_m)$ 与之对应，则称此对应为一个 $(n,m)$ 逻辑函数，记为 $\boldsymbol{Y}=F(x_1,x_2,\cdots,x_n)$，称 $n$ 为输入维数，$m$ 为输出维数。当 $m=1$ 时，称 $F$ 为单输出逻辑函数，简称逻辑函数；当 $m>1$ 时，称 $F$ 为多输出逻辑函数。其中 $F_2^t$ 是二元域 $F_2$ 上的 $t$ 维向量空间，任意的 $(x_1,x_2,\cdots,x_t)\in F_2^t$，向量 $(x_1,x_2,\cdots,x_t)$ 与其十进制值 $x_12^{t-1}+x_22^{t-2}+\cdots+x_t2^0$ 一一对应，为方便计，下文常用其十进制值表示向量 $(x_1,x_2,\cdots,x_t)$。

多输出逻辑函数在密码实践中有着广泛的应用，如序列密码中的多比特输出密钥序列发生器，每拍的输出可以看成是其对应状态的多输出逻辑函数；对明文按比特进行分组的分组密码中，明文分组与相应的密文分组之间的对应关系也可以看成多输出逻辑函数。密码体制中逻辑函数的相关免疫性是衡量该体制安全性的重要指标。相关免疫的阶数与相关攻击的计算复杂度密切相关，若使用相关免疫性弱的函数作为密码函数，则该密码体制易受相关分析法的攻击。关于单输出逻辑函数的相关免疫性已经有了广泛而深入的讨论，但对于多输出逻辑函数的相关免疫性，目前比较深入的研究结果尚不多见。文献 [1, 2] 引入了多输出相关免疫函数的概念 (文献 [1] 称为第 I 类多输出相关免疫函数)，它是单输出相关免疫函数概念的直接推广。文献 [3] 引入了另一类多输出相关免疫函数的概念，称为第 II 类多输出相关免疫函数，它把多输出函数的相关免疫性与分量函数的相关免疫性直接建立起了联系，并证明了第 I 类多输出相关免疫函数是第 II 类多输出相关免疫函数的子类。

本文对这两种多输出逻辑函数相关免疫性的刻划进行了更进一步的讨论，在用 Walsh 变换理论导出二元随机向量概率分布分解式的基础上，证明了这两种刻划的等价性，从而把多输出逻辑函数的相关免疫性与单输出逻辑函数的相关免疫性直接建立起了联系，并在第 4 节中利用多输出相关免疫逻辑函数构造了一类可以防止相关攻击和最佳线性逼近攻击的密钥流生成器。

## 2 两种多输出逻辑函数相关免疫性的刻划

首先引入单输出相关免疫逻辑函数的概念。

**定义 1**[1] 设 $f$ 是 $F_2^n$ 上的逻辑函数，$\boldsymbol{X}=(x_1,x_2,\cdots,x_n)$ 是二元域 $F_2$ 上 $n$ 个独立同分布的随机变量，它们都服从均匀分布。如果对任意满足 $|T|=t$ 的 $T=\{j_1,j_2,\cdots,j_t\}\subseteq\{1,2,\cdots,n\}$，随机变量 $y=f(x_1,x_2,\cdots,x_n)$ 与 $(x_{j_1},x_{j_2},\cdots,x_{j_t})$ 相互独立，即对任意 $(a_1,a_2,\cdots,a_t)\in F_2^t$ 和任意 $c\in F_2$，$\mathrm{Prob}\{y=c|x_{j_i}=a_i,1\le i\le t\}=\mathrm{Prob}\{y=c\}$，则称 $f$ 是 $(n,1,t)$ 相关免疫函数，或称 $f$ 是 $F_2^n$ 上的 $t$ 阶相关免疫函数。

[1] 2000-09-25 收到，2001-04-23 定稿

国家攀登计划 973 项目基金资助 (G1999035808)，国家自然科学基金项目 (A60173015)

**引理 1**[1] (Xiao-Messy) 逻辑函数 $f(\boldsymbol{X})$, $\boldsymbol{X}\in F_2^n$ 是 $t$ 阶相关免疫函数 $(1\le t<n)\Leftrightarrow$ 对任意 $\boldsymbol{\omega}\in F_2^n$，其 Hamming 重量 $1\le W(\boldsymbol{\omega})\le t$，都有 $\mathrm{Prob}\{f(\boldsymbol{X})=\boldsymbol{\omega}\boldsymbol{X}\}=0.5$。

其次，引入第 I 类多输出相关免疫函数的概念。

**定义 2**[1] 设 $F$ 是从 $F_2^n$ 到 $F_2^m$ 的函数，$x_1,x_2,\cdots,x_n$ 是二元域 $F_2$ 上 $n$ 个服从均匀分布并且相互独立的随机变量，如果对任意满足 $|T|=t$ 的 $T\{j_1,j_2,\cdots,j_t\}\subseteq\{1,2,\cdots,n\}$，随机变量 $\boldsymbol{y}=F(x_1,x_2,\cdots,x_n)$ 与 $(x_{j_1},x_{j_2},\cdots,x_{j_t})$ 相互独立，即对任意 $(a_1,a_2,\cdots,a_t)\in F_2^t$ 和任意 $\boldsymbol{c}\in F_2^n$，$\mathrm{Prob}\{\boldsymbol{y}=\boldsymbol{c}|x_{j_i}=a_i,\ 1\le i\le t\}=\mathrm{Prob}\{\boldsymbol{y}=\boldsymbol{c}\}$，则称 $F$ 是 $(n,m,t)$ 第 I 类多输出相关免疫函数。

最后，给出文献 [3] 中的第 II 类多输出相关免疫函数的概念。

**定义 3**[3] 设 $\boldsymbol{F}=(f_1,f_2,\cdots,f_m)$ 是从 $F_2^n$ 到 $F_2^m$ 的函数，如果 $\boldsymbol{F}$ 的分量函数的每一个非零线性组合 $f(\boldsymbol{X})=\oplus_{i=1}^m c_i f_i(\boldsymbol{X})$ 都是 $(n,l,t)$ 相关免疫函数，则称 $\boldsymbol{F}$ 是 $(n,m,t)$ 第 II 类多输出相关免疫函数，其中 $\boldsymbol{X}\in F_2^n$，$c_1,c_2,\cdots,c_m\in F_2$ 并且不全为零。

## 3 等价定理

一个二进制变元实值函数 $g$，是指对任意的 $\boldsymbol{X}\in F_2^n$ 都有唯一的 $g(\boldsymbol{X})\in R$ 与之对应，记为 $g:F_2^n\to R$，其中，$n$ 称为 $g$ 的元数，$R$ 是实数集合。任何一个二进制变元实值函数 $g(\boldsymbol{X})$ 都可用 Walsh 函数系展开为

$$g(\boldsymbol{X})=2^{-n}\sum_{\boldsymbol{\omega}\in F_2^n}S_g(\boldsymbol{\omega})(-1)^{\boldsymbol{\omega}\cdot\boldsymbol{X}} \tag{1}$$

其中

$$S_g(\boldsymbol{\omega})=\sum_{\boldsymbol{X}\in F_2^n}g(\boldsymbol{X})(-1)^{\boldsymbol{\omega}\cdot\boldsymbol{X}} \tag{2}$$

这里，$\boldsymbol{\omega}\cdot\boldsymbol{X}=\omega_1x_1\oplus\omega_2x_2\oplus\cdots\oplus\omega_nx_n$，$\boldsymbol{\omega}=(\omega_1,\omega_2,\cdots,\omega_n)\in F_2^n$，$\boldsymbol{X}=(x_1,x_2,\cdots,x_n)\in F_2^n$。(2) 式称为 Walsh 变换，对应的集合 $\{S_g(\boldsymbol{\omega}):\boldsymbol{\omega}\in F_2^n\}$ 称为 Walsh 谱。

利用 Walsh 谱和 Walsh 变换容易导出下面引理。

**引理 2(分解引理)** 设 $\boldsymbol{\xi}=(\xi_1,\xi_2,\cdots,\xi_m)$ 是 $F_2$ 上的 $m$ 维随机向量，$\boldsymbol{a}\in F_2^m$，则有

$$\mathrm{Prob}\{\boldsymbol{\xi}=\boldsymbol{a}\}=\frac{1}{2^{m-1}}\sum_{\boldsymbol{\omega}=1}^{2^m-1}\mathrm{Prob}\{\boldsymbol{\omega}\cdot\boldsymbol{\xi}=\boldsymbol{\omega}\cdot\boldsymbol{a}\}+\frac{1}{2^{m-1}}-1 \tag{3}$$

**证明** $m$ 维随机向量 $\boldsymbol{\xi}=(\xi_1,\xi_2,\cdots,\xi_m)$ 的概率分布 $\mathrm{Prob}\{\boldsymbol{\xi}=\boldsymbol{X}\}$ 是一个 $F_2^n$ 到实数集 $R$ 上的二进制变元实值函数，记为 $g(\boldsymbol{X})=\mathrm{Prob}\{\boldsymbol{\xi}=\boldsymbol{X}\}$，其 Walsh 变换为

$$S_g(\boldsymbol{\omega})=\sum_{\boldsymbol{X}\in F_2^n}(-1)^{\boldsymbol{\omega}\cdot\boldsymbol{X}}\mathrm{Prob}\{\boldsymbol{\xi}=\boldsymbol{X}\}$$

显然，$S_g(\boldsymbol{\omega})$ 的概率意义为

$$S_g(\boldsymbol{\omega})=\mathrm{Prob}\{\boldsymbol{\omega}\cdot\boldsymbol{\xi}=0\}-\mathrm{Prob}\{\boldsymbol{\omega}\cdot\boldsymbol{\xi}=1\}=2\mathrm{Prob}\{\boldsymbol{\omega}\cdot\boldsymbol{\xi}=0\}-1$$

由 (1) 式，有

$$\begin{aligned}\mathrm{Prob}\{\boldsymbol{\xi}=\boldsymbol{a}\}&=\frac{1}{2^m}\sum_{\boldsymbol{\omega}=0}^{2^m-1}(-1)^{\boldsymbol{\omega}\cdot\boldsymbol{a}}S_g(\boldsymbol{\omega})=\frac{1}{2^m}\sum_{\boldsymbol{\omega}=0}^{2^m-1}(-1)^{\boldsymbol{\omega}\cdot\boldsymbol{a}}(2\mathrm{Prob}\{\boldsymbol{\omega}\cdot\boldsymbol{\xi}=0\}-1)\\&=\frac{1}{2^{m-1}}\sum_{\boldsymbol{\omega}=0}^{2^m-1}(-1)^{\boldsymbol{\omega}\cdot\boldsymbol{a}}\mathrm{Prob}\{\boldsymbol{\omega}\cdot\boldsymbol{\xi}=0\}-\frac{1}{2^m}\sum_{\boldsymbol{\omega}=0}^{2^m-1}(-1)^{\boldsymbol{\omega}\cdot\boldsymbol{a}}\end{aligned}$$

当 $\boldsymbol{a}=0$ 时，有

$$\begin{aligned}\mathrm{Prob}\{\boldsymbol{\xi}=0\}&=\frac{1}{2^{m-1}}\sum_{\boldsymbol{\omega}=\boldsymbol{0}}^{2^m-1}\mathrm{Prob}\{\boldsymbol{\omega}\cdot\boldsymbol{\xi}=0\}-1\\&=\frac{1}{2^{m-1}}\sum_{\boldsymbol{\omega}=1}^{2^m-1}\mathrm{Prob}\{\boldsymbol{\omega}\cdot\boldsymbol{\xi}=0\}+\frac{1}{2^{m-1}}-1\end{aligned}$$

当 $\boldsymbol{a}\neq 0$ 时，由于 $\sum_{\boldsymbol{\omega}=0}^{2^m-1}(-1)^{\boldsymbol{\omega}\cdot\boldsymbol{a}}=0$ 及

$$(-1)^{\boldsymbol{\omega}\cdot\boldsymbol{a}}\mathrm{Prob}\{\boldsymbol{\omega}\cdot\boldsymbol{\xi}=0\}=\mathrm{Prob}\{\boldsymbol{\omega}\cdot\boldsymbol{\xi}=\boldsymbol{\omega}\cdot\boldsymbol{a}\}-\boldsymbol{\omega}\cdot\boldsymbol{a}$$

其中 $\boldsymbol{\omega}\cdot\boldsymbol{a}$ 作为 0, 1 实数参与等式右边的运算，故

$$\begin{aligned}\mathrm{Prob}\{\boldsymbol{\xi}=\boldsymbol{a}\}&=\frac{1}{2^{m-1}}\sum_{\boldsymbol{\omega}=0}^{2^m-1}(\mathrm{Prob}\{\boldsymbol{\omega}\cdot\boldsymbol{\xi}=\boldsymbol{\omega}\cdot\boldsymbol{a}\}-\boldsymbol{\omega}\cdot\boldsymbol{a})\\&=\frac{1}{2^{m-1}}\sum_{\boldsymbol{\omega}=0}^{2^m-1}\mathrm{Prob}\{\boldsymbol{\omega}\cdot\boldsymbol{\xi}=\boldsymbol{\omega}\cdot\boldsymbol{a}\}-\frac{1}{2^{m-1}}\sum_{\boldsymbol{\omega}=0}^{2^m-1}\boldsymbol{\omega}\cdot\boldsymbol{a}\\&=\frac{1}{2^{m-1}}\sum_{\boldsymbol{\omega}=1}^{2^m-1}\mathrm{Prob}\{\boldsymbol{\omega}\cdot\boldsymbol{\xi}=\boldsymbol{\omega}\cdot\boldsymbol{a}\}+\frac{1}{2^{m-1}}-1\end{aligned}$$

因此，对任意 $\boldsymbol{a}\in F_2^m$，引理 2 成立。　　证毕

**引理 3**　设 $\boldsymbol{\eta}=(\eta_1,\eta_2,\cdots,\eta_t)$ 是 $F_2$ 上的 $t$ 维随机向量，$\boldsymbol{\xi}=(\xi_1,\xi_2,\cdots,\xi_m)$ 是 $F_2$ 上的 $m$ 维随机向量，则 $\boldsymbol{\eta}$ 与 $\boldsymbol{\xi}=(\xi_1,\xi_2,\cdots,\xi_m)$ 相互独立 $\Leftrightarrow$ $\boldsymbol{\eta}$ 与 $\xi_1,\xi_2,\cdots,\xi_m$ 的每一个非零线性组合 $\oplus_{i=1}^m c_i\xi_i$ 相互独立，其中 $c_1,c_2,\cdots,c_m\in F_2$，并且不全为零。

**证明**　“ $\Rightarrow$ ” 对任意 $c_1,c_2,\cdots,c_m\in F_2$，并且不全为零，$\boldsymbol{c}\in F_2$，记

$$\tau_c(c_1,c_2,\cdots,c_m)=\{\boldsymbol{\beta}|\boldsymbol{\beta}=(\beta_1,\beta_2,\cdots,\beta_m)\in F_2^m,\ \mathop{\oplus}_{i=1}^{m}c_i\beta_i=c\}$$

由条件，有

$$\begin{aligned}\mathrm{Prob}\left\{\mathop{\oplus}_{i=1}^{m}c_i\xi_i=c|\boldsymbol{\eta}=\boldsymbol{b}\right\}&=\sum_{\boldsymbol{\beta}\in\tau_c(c_1,c_2,\cdots,c_m)}\mathrm{Prob}\{\boldsymbol{\xi}=\boldsymbol{\beta}|\boldsymbol{\eta}=\boldsymbol{b}\}\\&=\sum_{\boldsymbol{\beta}\in\tau_c(c_1,c_2,\cdots,c_m)}\mathrm{Prob}\{\boldsymbol{\xi}=\boldsymbol{\beta}\}=\mathrm{Prob}\left\{\mathop{\oplus}_{i=1}^{m}c_i\xi_i=c\right\}\end{aligned}$$

其中 $\boldsymbol{b}=(b_1,b_2,\cdots,b_t)\in F_2^t$。

“ $\Leftarrow$ ” 由条件 $\mathrm{Prob}\{\boldsymbol{\omega}\cdot\boldsymbol{\xi}=\boldsymbol{\omega}\cdot\boldsymbol{a}|\boldsymbol{\eta}=\boldsymbol{b}\}=\mathrm{Prob}\{\boldsymbol{\omega}\cdot\boldsymbol{\xi}=\boldsymbol{\omega}\cdot\boldsymbol{a}\}$ 及引理 2，有

$$\begin{aligned}\mathrm{Prob}\{\boldsymbol{\xi}=\boldsymbol{a}|\boldsymbol{\eta}=\boldsymbol{b}\}&=\frac{1}{2^{m-1}}\sum_{\boldsymbol{\omega}=1}^{2^m-1}\mathrm{Prob}\{\boldsymbol{\omega}\cdot\boldsymbol{\xi}=\boldsymbol{\omega}\cdot\boldsymbol{a}|\boldsymbol{\eta}=\boldsymbol{b}\}+\frac{1}{2^{m-1}}-1\\&=\frac{1}{2^{m-1}}\sum_{\boldsymbol{\omega}=1}^{2^m-1}\mathrm{Prob}\{\boldsymbol{\omega}\cdot\boldsymbol{\xi}=\boldsymbol{\omega}\cdot\boldsymbol{a}\}+\frac{1}{2^{m-1}}-1=\mathrm{Prob}\{\boldsymbol{\xi}=\boldsymbol{a}\}\end{aligned}$$

因此， $\eta$ 与 $\xi$ 相互独立。 证毕

**定理 1(等价定理)** 设 $\boldsymbol{F}=(f_1,f_2,\cdots,f_m)$ 是从 $F_2^n$ 到 $F_2^m$ 的函数，设 $x_1,x_2,\cdots,x_n$ 是二元域 $F_2$ 上的 $n$ 个服从均匀分布并且相互独立的随机变量，则 $\boldsymbol{F}$ 是 $(n,m,t)$ 第 II 类多输出相关免疫函数 $\Leftrightarrow$ $\boldsymbol{F}$ 是 $(n,m,t)$ 第 I 类多输出相关免疫函数。

**证明** 由定义 2 、定义 3 及引理 3 知， $\boldsymbol{F}$ 是 $(n,m,t)$ 第 I 类多输出相关免疫函数 $\Leftrightarrow$ 对任意 $\{j_1,j_2,\cdots,j_t\}\subseteq\{1,2,\cdots,n\}$ ，随机变量

$$\boldsymbol{y}=\boldsymbol{F}(x_1,x_2,\cdots,x_n)=(y_1,y_2,\cdots,y_m)$$

与 $(x_{j_1},x_{j_2},\cdots,x_{j_t})$ 相互独立。 $\Leftrightarrow$ 对任意 $\{j_1,j_2,\cdots,j_t\}\subseteq\{1,2,\cdots,n\}$, $(y_1,y_2,\cdots,y_m)$ 的每个非零线性组合

$$\bigoplus_{i=1}^{m}c_iy_i=\bigoplus_{i=1}^{m}c_if_i(x_1,x_2,\cdots,x_n)$$

与 $(x_{j_1},x_{j_2},\cdots,x_{j_t})$ 相互独立。 $\Leftrightarrow$ $\boldsymbol{F}$ 分量函数的每个非零线性组合 $\oplus_{i=1}^{m}c_if_i(X)$ 都是 $(n,l,t)$ 相关免疫函数 (其中 $\boldsymbol{X}\in F_2^n$), $\Leftrightarrow$ $\boldsymbol{F}=(f_1,f_2,\cdots,f_m)$ 是 $(n,m,t)$ 第 II 类多输出相关免疫函数。 证毕

由等价定理及 Xiao-Messy 引理知，密码分析中我们在考察多输出逻辑函数的相关优势时，应当考察输出分位函数所有线性组合的输入输出相关优势，而不仅仅考察其单个分位函数的输入输出相关优势。

## 4 在密钥流生成器设计中的应用

在序列密码中常采用图 1 中的一类密钥流生成器，称为非线性组合生成器。此类生成器中各线性反馈移存器的初态由密钥预置。这类生成器作为密钥流生成器不仅结构简单易于工程实现，而且输出的密钥流序列具有较好的伪随机特性，对输出序列的线性复杂度也易于估计，因此，非线性组合生成器是一类较理想的密钥流生成器。尽管如此，但在构造此类密钥流生成器时，逻辑函数 $f$ 必须经过慎重选择，否则，容易由逻辑函数的最佳仿射逼近来求取密钥 (各 FSR 的初态) 。然而，由逻辑函数谱值理论易知，无论 $f$ 取何种逻辑函数，一定存在输入序列的某种线性组合与输出的密钥流有一定的符合优势，即

$$\mathrm{Prob}\{f(x_1,x_2,\cdots,x_n)=\bigoplus_{i=1}^{m}c_ix_i\}>0.5 \quad 或 \quad \mathrm{Prob}\{f(x_1,x_2,\cdots,x_n)=\bigoplus_{i=1}^{m}c_ix_i\}<0.5$$

对 $f$ 的精心选择只能做到把这种不平衡性尽量均匀地分配到不同的输入变元线性组合中，而不能根本消除它。

多输出相关免疫逻辑函数在此类密钥流生成器中的应用将改变这种状况，使得由密钥流符号求取各 FSR 的初态更加困难。为说明这点，我们构造一类利用多输出相关免疫逻辑函数的密钥流生成器，如图 2 所示。其中 $\boldsymbol{F}(\boldsymbol{X})=(f_1,f_2,\cdots,f_n,f_{n+1},\cdots,f_{n+t})$ 是 $(n+t,n+t,n)$ 平衡的多输出相关免疫逻辑函数， $f_1,f_2,\cdots,f_n$ 作为密钥流生成器的输出符号， $f_{n+1},f_{n+2},\cdots,f_{n+t}$ 延迟一拍作为下一节拍函数 $\boldsymbol{F}(\boldsymbol{X})$ 的 $t$ 个输入符号，其余 $n$ 个输入符号由 $n$ 个线性移存器的同拍输出提供。由第 3 节中的等价定理可以看到，该密钥流生成器输出符号 $f_1,f_2,\cdots,f_n$ 的任意线性组合 $\oplus_{i=1}^{n}c_if_i$ 与各 FSR 的输出符号 $x_1,x_2,\cdots,x_n$ 的任意线性组合 $\oplus_{i=1}^{n}c_ix_i$ 之间都满足

$$\mathrm{Prob}\left\{\bigoplus_{i=1}^{n}c_if_i=\bigoplus_{i=1}^{n}c_ix_i\right\}=0.5$$

即密钥流生成器输出符号 $f_1, f_2, \cdots, f_n$ 与 $x_1, x_2, \cdots, x_n$ 是统计独立的。这样，可以避免利用相关攻击或线性逼近攻击来求取各 FSR 的初态 (密钥)。

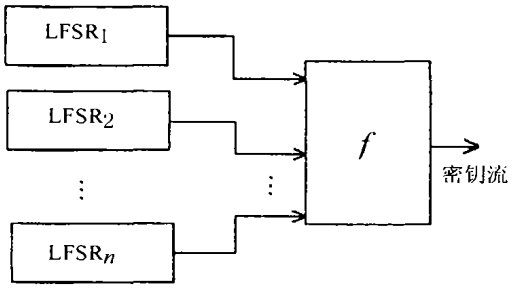


图 1　非线性组合生成器，$f$ 是非线性逻辑函数

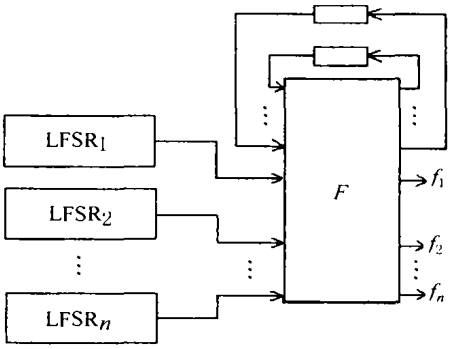


图 2　利用多输出相关免疫函数的非线性组合生成器

当然，在构造此类密钥流生成器时，首先应当使各 FSR 的级数足够大，以避免对该生成器的强力攻击；其次，多输出相关免疫逻辑函数 $\boldsymbol{F}(\boldsymbol{X})$ 的选取必须使得 $\boldsymbol{F}(\boldsymbol{X})$ 的各维输出函数具有相当的非线性次数，以及密钥流生成器输出序列具有足够的线性复杂度。关于平衡的多输出相关免疫逻辑函数的构造问题在此不作讨论，具体构造方法可参考文献 [3]。

## 参　考　文　献

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

[2] K. Gopalakrishnan, D. R. Stinson, Three charaterizations of non-binary correlation-immune and resilient functions, Designs, Codes and Cryptography, 1995, 5(3), 241–251.

[3] 陈鲁生，多输出布尔函数的密码学性质，[博士论文]，天津，南开大学，2000.

# EQUIVALENT CHARACTERIZATION AND APPLICATION OF MULTI-OUTPUT CORRELATION-IMMUNE BOOLEAN FUNCTION

Xu Hanliang　　Lü Shuwang

(*State Key Lab of Information Security, Graduate School of CAS, Beijing* 100039, *China*)

**Abstract**　This paper discusses the characterizations of multi-output correlation-immune functions. We first give a decomposition formula of the probability distribution of binary random vectors by using Walsh transform. Then the equivalence of the two different definitions of multi-output correlation-immune functions is proved. Furthermore, a class of keystream generators is constructed which can resist the linear and correlation attacks.

**Key words**　Multi-output logical function, Correlation-immunity, Walsh transform, Equivalent theorem, Keystream generator

徐汉良：　男，1964 年生，博士，主要研究方向：密码算法，信息安全.

吕述望：　男，1941 年生，教授，主要研究方向：密码与信息安全技术.