学术论文

# 与特定密码函数线性等价的布尔函数谱和自相关特征

杨　锐，曾本胜，李世取
（解放军信息工程学院信息研究系，郑州　450002）

[摘要]　对线性等价意义下 2 个布尔函数的密码学性质的异同做了进一步的分析，得到了一个布尔函数线性等价于某个具有 $m$ 阶相关免疫性的布尔函数的充分必要条件和线性等价于某个满足 $k$ 次扩散准则的布尔函数的充分必要条件，在线性等价意义上，给出了由不具有相关免疫性且不满足扩散准则的布尔函数，构造既具有相关免疫性、也满足扩散准则的布尔函数的实例。

[关键词]　线性等价；Walsh 循环谱；自相关函数；相关免疫性；扩散准则；SAC
[中图分类号]　TN918.1　　[文献标识码]　A　　[文章编号]　1009－1742（2005）11－0060－06

## 1　引言

线性等价的定义是由文献［1］给出的。随后，构造线性等价意义下的满足一定密码学性质的布尔函数受到了广大学者的关注，如在文献[2]中直接分析了线性等价意义下布尔函数某些密码学性质的变化，指出了在变量的可逆线性变换的作用下（即线性等价意义下），函数的代数次数、平衡性、非线性度及满足扩散准则的点个数保持不变（即不变性），同时给出了线性等价意义下构造平衡的、满足高次扩散准则的布尔函数的方法。后来在文献[3]中给出了从一个不具有相关免疫性的平衡布尔函数出发，构造线性等价意义下一阶弹性函数的方法，此方法也正是文献[4]中所提到的 LT 方法。温巧燕、钮心忻、杨义先教授指出，非线性、平衡性、相关免疫性和扩散性是衡量密码函数性能优劣的重要指标，构造平衡、满足扩散准则且具有足够高非线性度的相关免疫函数是一个重要的研究课题[5]。基于此，特别是注意到密钥流非线性组合器的设计需综合考虑各种优良性的发展趋势，笔者首先用概率方法给出了线性等价的两个布尔函数的 Walsh 循环谱及自相关函数之间的关系，由此得到了一个布尔函数线性等价于某个具有 $m$ 阶相关免疫性的布尔函数的充分必要条件和线性等价于某个满足 $k$ 次扩散准则的布尔函数的充分必要条件，也就给出了一个布尔函数线性等价于某个既具有 $m$ 阶相关免疫性且满足 $k$ 次扩散准则的布尔函数的充分必要条件和相应的构造方法。作为应用，笔者由既不具有相关免疫性、也不满足 SAC 的 5 元布尔函数出发，构造了与其线性等价的既具有相关免疫性、也满足 SAC 的五元布尔函数。而文献[2, 3]中的有关分析结果只是笔者的有关定理的特殊情况，且文献[2]中的构造仅是针对扩散准则，文献[3]中的构造仅是针对一阶相关免疫性的，在一定意义上，笔者对以往的有关分析工作做了理论升华，并进一步考虑了用于密钥流非线性组合生成器的布尔函数的综合优良性问题。

## 2　基本概念

凡 $\boldsymbol{x}$ 都表示

$$\boldsymbol{x} = (x_1, x_2, \cdots, x_n) \in \mathrm{GF}^n(2),$$

凡 $\boldsymbol{X}$ 都表示

$$\boldsymbol{X} = (X_1, X_2, \cdots, X_n),$$

其中 $X_1, X_2, \cdots, X_n$ 是定义在某概率空间$(\Omega, F,$

[收稿日期]　2004－07－26；修回日期　2004－09－18
[作者简介]　杨　锐（1980－），男，湖北武汉市人，解放军信息工程大学信息工程学院硕士研究生

$P$) 上相互独立的 $n$ 个布尔随机变量，且分布均匀：

$$P\{X_i = 0\} = P\{X_i = 1\} = 1/2, 1 \leqslant i \leqslant n。$$

记二元域为 GF (2)，布尔函数、点积 $\boldsymbol{w} \cdot \boldsymbol{x}$、汉明重量为 $W(\boldsymbol{w})$、Walsh 循环谱 $S_{(f)}(\boldsymbol{w})$、自相关函数 $r_f(\boldsymbol{s})$、布尔函数相关免疫、扩散准则的定义见文献[6]。

**定义 1**[1]　称 $n$ 元布尔函数 $g(\boldsymbol{x})$ 和 $f(\boldsymbol{x})$ 在线性变换意义下是等价的 —— 简称为线性等价，如果存在 GF(2) 上的 $n \times n$ 可逆矩阵 $\boldsymbol{A}$ 和 $\boldsymbol{a}$，$\boldsymbol{b} \in \mathrm{GF}^n(2)$ 及 $c \in \mathrm{GF}(2)$，使得

$$g(\boldsymbol{x}) = f(\boldsymbol{xA} + \boldsymbol{a}) + \boldsymbol{b} \cdot \boldsymbol{x} + c,\ \boldsymbol{x} \in \mathrm{GF}^n(2) \tag{1}$$

**定义 2**[7]　称布尔函数 $f(\boldsymbol{x}), \boldsymbol{x} \in \mathrm{GF}^n(2)$ 是满足 $k$ ($k \geqslant 1$ 为正整数) 次扩散准则的，若对所有的 $\boldsymbol{s} \in \mathrm{GF}^n(2), 1 \leqslant W(\boldsymbol{s}) \leqslant k$，其自相关函数 $r_f$ 满足

$$r_f(\boldsymbol{s}) = 0。$$

特别称满足 1 次扩散准则的布尔函数是满足 SAC 的。

**引理 1**[8]　设 $f(\boldsymbol{x}), \boldsymbol{x} \in \mathrm{GF}^n(2)$ 是任一布尔函数，则有

$$S_{(f)}(\boldsymbol{w}) = 2P\{f(\boldsymbol{X}) + \boldsymbol{w} \cdot \boldsymbol{X} = 0\} - 1,\quad \boldsymbol{w} \in \mathrm{GF}^n(2)。$$

**引理 2**[6]　设 $f(\boldsymbol{x}), \boldsymbol{x} \in \mathrm{GF}^n(2)$ 是任一布尔函数，则有

$$r_f(\boldsymbol{s}) = 2P\{f(\boldsymbol{X} + \boldsymbol{s}) + f(\boldsymbol{X}) = 0\} - 1,\quad \boldsymbol{s} \in \mathrm{GF}^n(2)。$$

**引理 3**[9]　布尔函数 $f(\boldsymbol{x})$，$\boldsymbol{x} \in \mathrm{GF}^n(2)$ 是 $m$ 阶相关免疫的充分必要条件是对所有的 $\boldsymbol{w} \in \mathrm{GF}^n(2), 1 \leqslant W(\boldsymbol{w}) \leqslant m$，都有 $S_{(f)}(\boldsymbol{w}) = 0$。

引理 1 和引理 2 分别是布尔函数 Walsh 循环谱和自相关函数的概率表示式，引理 3 是著名的 Xiao-massey 定理。

## 3　主要结果

### 3.1　线性等价的两个布尔函数的 Walsh 循环谱之间的关系和自相关函数之间的关系

**引理 4**　设 $n$ 元布尔函数 $g(\boldsymbol{x})$ 和 $f(\boldsymbol{x})$ 线性等价，即存在 GF(2) 上的 $n \times n$ 可逆矩阵 $\boldsymbol{A}$ 和 $\boldsymbol{a}$，$\boldsymbol{b} \in \mathrm{GF}^n(2)$ 及 $c \in \mathrm{GF}(2)$，使 $g(\boldsymbol{x}) = f(\boldsymbol{xA} + \boldsymbol{a}) + \boldsymbol{b} \cdot \boldsymbol{x} + c, \boldsymbol{x} \in \mathrm{GF}^n(2)$，则 $g(\boldsymbol{x})$ 的 Walsh 循环谱 $S_{(g)}(\cdot)$ 和 $f(\boldsymbol{x})$ 的 Walsh 循环谱 $S_{(f)}(\cdot)$ 有下述关系：

$$S_{(g)}(\boldsymbol{w}) = (-1)^{c + \boldsymbol{a}\boldsymbol{A}^{-1}(\boldsymbol{w}+\boldsymbol{b})^{\mathrm{T}}} \cdot S_{(f)}((\boldsymbol{w} + \boldsymbol{b})(\boldsymbol{A}^{-1})^{\mathrm{T}}), \boldsymbol{w} \in \mathrm{GF}^n(2) \tag{2}$$

**证明**　根据引理 1 和点积的定义，并注意到 $\boldsymbol{Y} = \boldsymbol{XA} + \boldsymbol{a}$ 仍是相互独立且都具有均匀分布的 $n$ 维布尔随机向量，即知

$$\begin{aligned}
S_{(g)}(\boldsymbol{w}) &= 2P\{g(\boldsymbol{X}) = \boldsymbol{w} \cdot \boldsymbol{X}\} - 1 = \\
&2P\{f(\boldsymbol{XA} + \boldsymbol{a}) + \boldsymbol{b} \cdot \boldsymbol{X} + c = \boldsymbol{w} \cdot \boldsymbol{X}\} - 1 = \\
&2P\{f(\boldsymbol{Y}) + c = \boldsymbol{X}(\boldsymbol{AA}^{-1})(\boldsymbol{w} + \boldsymbol{b})^{\mathrm{T}}\} - 1 = \\
&2P\{f(\boldsymbol{Y}) + c = [(\boldsymbol{XA} + \boldsymbol{a} + \boldsymbol{a})\boldsymbol{A}^{-1}(\boldsymbol{w} + \boldsymbol{b})^{\mathrm{T}}]\} - \\
&1 = 2P\{f(\boldsymbol{Y}) + c = [(\boldsymbol{XA} + \boldsymbol{a})\boldsymbol{A}^{-1}(\boldsymbol{w} + \boldsymbol{b})^{\mathrm{T}} + \\
&\boldsymbol{a}\boldsymbol{A}^{-1}(\boldsymbol{w} + \boldsymbol{b})^{\mathrm{T}}]\} - 1 = 2P\{f(\boldsymbol{Y}) + c = \\
&[\boldsymbol{Y}\boldsymbol{A}^{-1}(\boldsymbol{w} + \boldsymbol{b})^{\mathrm{T}} + \boldsymbol{a}\boldsymbol{A}^{-1}(\boldsymbol{w} + \boldsymbol{b})^{\mathrm{T}}]\} - 1 = \\
&2P\{f(\boldsymbol{Y}) + c = [(\boldsymbol{w} + \boldsymbol{b})(\boldsymbol{A}^{-1})^{\mathrm{T}}]\boldsymbol{Y}^{\mathrm{T}} + \\
&\boldsymbol{a}\boldsymbol{A}^{-1}(\boldsymbol{w} + \boldsymbol{b})^{\mathrm{T}}\} - 1 = 2P\{f(\boldsymbol{X}) = \\
&[(\boldsymbol{w} + \boldsymbol{b})(\boldsymbol{A}^{-1})^{\mathrm{T}}] \cdot \boldsymbol{X} + \boldsymbol{a}\boldsymbol{A}^{-1}(\boldsymbol{w} + \boldsymbol{b})^{\mathrm{T}} + c\} - \\
&1 = (-1)^{c + \boldsymbol{a}\boldsymbol{A}^{-1}(\boldsymbol{w}+\boldsymbol{b})^{\mathrm{T}}} S_{(f)}((\boldsymbol{w} + \boldsymbol{b})(\boldsymbol{A}^{-1})^{\mathrm{T}}), \\
&\boldsymbol{w} \in \mathrm{GF}^n(2),
\end{aligned}$$

因而式(2)成立。

特别取 $\boldsymbol{b} = 0 \in \mathrm{GF}^n(2), c = 1$，上述引理 4 的结论即为文献[8, 10]中的相关结论。

**引理 5**　设 $n$ 元布尔函数 $g(\boldsymbol{x})$ 和 $f(\boldsymbol{x})$ 线性等价，即存在 GF(2) 上的 $n \times n$ 可逆矩阵 $\boldsymbol{A}$ 和 $\boldsymbol{a}$，$\boldsymbol{b} \in \mathrm{GF}^n(2)$ 及 $c \in \mathrm{GF}(2)$，使有 $g(\boldsymbol{x}) = f(\boldsymbol{xA} + \boldsymbol{a}) + \boldsymbol{b} \cdot \boldsymbol{x} + c, \boldsymbol{x} \in \mathrm{GF}^n(2)$，则 $g(\boldsymbol{x})$ 的自相关函数 $r_g(\cdot)$ 和 $f(\boldsymbol{x})$ 的自相关函数 $r_f(\cdot)$ 有下述关系：

$$r_g(\boldsymbol{s}) = (-1)^{\boldsymbol{b} \cdot \boldsymbol{s}} r_f(\boldsymbol{sA}), \boldsymbol{s} \in \mathrm{GF}^n(2) \tag{3}$$

**证明**　根据引理 2 同样可知

$$\begin{aligned}
r_g(\boldsymbol{s}) &= 2P\{g(\boldsymbol{X} + \boldsymbol{s}) + g(\boldsymbol{X}) = 0\} - 1 = \\
&2P\{f((\boldsymbol{X} + \boldsymbol{s})\boldsymbol{A} + \boldsymbol{a}) + \boldsymbol{b} \cdot (\boldsymbol{X} + \boldsymbol{s}) + c + \\
&f(\boldsymbol{XA} + \boldsymbol{a}) + \boldsymbol{b} \cdot \boldsymbol{X} + c = 0\} - 1 = \\
&2P\{f((\boldsymbol{XA} + \boldsymbol{a}) + \boldsymbol{sA}) + \boldsymbol{b} \cdot \boldsymbol{s} + f(\boldsymbol{XA} + \boldsymbol{a}) = \\
&0\} - 1 = 2P\{f(\boldsymbol{Y} + \boldsymbol{sA}) + f(\boldsymbol{Y}) = \boldsymbol{b} \cdot \boldsymbol{s}\} - \\
&1 = 2P\{f(\boldsymbol{X} + \boldsymbol{sA}) + f(\boldsymbol{X}) = \boldsymbol{b} \cdot \boldsymbol{s}\} - 1 = \\
&(-1)^{\boldsymbol{b} \cdot \boldsymbol{s}} r_f(\boldsymbol{sA}),\ \boldsymbol{s} \in \mathrm{GF}^n(2),
\end{aligned}$$

因而式 (3) 成立。

### 3.2　线性等价意义下布尔函数性质的异同分析

根据上述引理 4 引理 5，可以清晰地分析线性等价的 2 个布尔函数有关性质的异同之处。

**定理 1**　设 $n$ 元布尔函数 $g(\boldsymbol{x})$ 和 $f(\boldsymbol{x})$ 线性等价，即存在 GF(2) 上的 $n \times n$ 可逆矩阵 $\boldsymbol{A}$ 和 $\boldsymbol{a}$，$\boldsymbol{b} \in \mathrm{GF}^n(2)$ 及 $c \in \mathrm{GF}(2)$，使有 $g(\boldsymbol{x}) = f(\boldsymbol{xA} + \boldsymbol{a}) + \boldsymbol{b} \cdot \boldsymbol{x} + c, \boldsymbol{x} \in \mathrm{GF}^n(2)$，记

$$\boldsymbol{S}_{f0} = \{\boldsymbol{w}:\boldsymbol{w} \in GF^n(2),\ S_{(f)}(\boldsymbol{w}) = 0\},$$

$$\boldsymbol{S}_{g0} = \{\boldsymbol{w}:\boldsymbol{w} \in GF^n(2),\ S_{(g)}(\boldsymbol{w}) = 0\},$$

则对 $\boldsymbol{w} \in GF^n(2)$，有

$$S_{(g)}(\boldsymbol{w}) = 0 \Leftrightarrow S_{(f)}((\boldsymbol{w}+\boldsymbol{b})(\boldsymbol{A}^{-1})^{\mathrm{T}}) = 0 \quad (4)$$

因而成立 $|\boldsymbol{S}_{f0}| = |\boldsymbol{S}_{g0}|$。

证明　根据引理4中式(2)，并注意到矩阵 $\boldsymbol{A}$ 可逆即得。

定理2　设 $n$ 元布尔函数 $g(\boldsymbol{x})$ 和 $f(\boldsymbol{x})$ 线性等价，即存在GF(2)上的 $n \times n$ 可逆矩阵 $\boldsymbol{A}$ 和 $\boldsymbol{a}$，$\boldsymbol{b} \in GF^n(2)$ 及 $c \in GF(2)$，使有 $g(\boldsymbol{x}) = f(\boldsymbol{x}\boldsymbol{A}+\boldsymbol{a}) + \boldsymbol{b}\cdot\boldsymbol{x} + c$，$\boldsymbol{x} \in GF^n(2)$，记 $f(\boldsymbol{x})$ 的全体线性结构之集[7]为 $\boldsymbol{U}_f$，$g(\boldsymbol{x})$ 的全体线性结构之集为 $\boldsymbol{U}_g$，又记

$$\boldsymbol{R}_{f0} = \{\boldsymbol{s}:\boldsymbol{s} \in GF^n(2), r_f(\boldsymbol{s}) = 0\},$$

$$\boldsymbol{R}_{g0} = \{\boldsymbol{s}:\boldsymbol{s} \in GF^n(2), r_g(\boldsymbol{s}) = 0\},$$

则对 $\boldsymbol{s} \in GF^n(2)$，有

$$|r_g(\boldsymbol{s}\boldsymbol{A}^{-1})| = 1 \Leftrightarrow |r_f(\boldsymbol{s})| = 1,$$

$$r_g(\boldsymbol{s}\boldsymbol{A}^{-1}) = 0 \Leftrightarrow r_f(\boldsymbol{s}) = 0,$$

因而成立

$$\boldsymbol{U}_g = \{\boldsymbol{s}\boldsymbol{A}^{-1}:\boldsymbol{s} \in \boldsymbol{U}_f\},\ \boldsymbol{R}_{g0} = \{\boldsymbol{s}\boldsymbol{A}^{-1}:\boldsymbol{s} \in \boldsymbol{R}_{f0}\},$$

于是还有 $|\boldsymbol{U}_g| = |\boldsymbol{U}_f|$，$|\boldsymbol{R}_{g0}| = |\boldsymbol{R}_{f0}|$。

证明　根据引理5中式(3)，并注意到矩阵 $\boldsymbol{A}$ 可逆，即得

$$r_g(\boldsymbol{s}\boldsymbol{A}^{-1}) = (-1)^{\boldsymbol{b}\cdot\boldsymbol{s}\boldsymbol{A}^{-1}} r_f(\boldsymbol{s}\boldsymbol{A}^{-1}\boldsymbol{A}) = (-1)^{\boldsymbol{b}\cdot\boldsymbol{s}\boldsymbol{A}^{-1}} r_f(\boldsymbol{s})。$$

定理1和定理2的结论告知，2个线性等价的布尔函数Walsh循环谱的零点个数相同、线性结构点的个数相同、扩散点——自相关函数取值为零的点个数也相同，但是它们Walsh循环谱的零点、线性结构点、扩散点又都可能不相同。

### 3.3 应用

根据定理1和定理2的结论易知，若取 $\boldsymbol{A}$ 为换位矩阵(每一行的汉明重量都为1的可逆矩阵)，则对任意的 $\boldsymbol{a} \in GF^n(2)$ 及 $c \in GF(2)$，布尔函数 $f(\boldsymbol{x})$ 和与其线性等价的布尔函数 $g(\boldsymbol{x}) = f(\boldsymbol{x}\boldsymbol{A}+\boldsymbol{a}) + c$ 有完全相同的相关免疫性——都不具有或同为 $m$ 阶相关免疫的和完全相同的扩散特性——都不具有或同满足 $k$ 次扩散准则。不仅如此，应用前面的分析结果，可以将某些不具有相关免疫性但满足适定条件的布尔函数线性变换为相关免疫的布尔函数，且可将某些不具有扩散性但满足适定条件的布尔函数线性变换为满足扩散准则的布尔函数，还可将某些既不具有相关免疫性也不满足扩散准则的布尔函数线性变换为既具有某阶相关免疫性、也满足某次扩散准则的布尔函数。为此，再给出有关条件：

以 $\boldsymbol{w}(i) \in GF^n(2)$ 表示只有第 $i$ 个分量取值为1的 $n$ 维布尔向量，$1 \leqslant i \leqslant n$，…。一般地，以 $\boldsymbol{w}(i_1, \cdots, i_k) \in GF^n(2)$ 表示只有第 $i_1$ 个分量、……、第 $i_k$ 个分量取值为1的 $n$ 维布尔向量，$1 \leqslant i_1 < \cdots < i_k \leqslant n$，$1 \leqslant k \leqslant n-1$，则有

定理3　设 $f(\boldsymbol{x})$，$\boldsymbol{x} \in GF^n(2)$ 是 $n$ 元布尔函数，$S_{(f)}(\boldsymbol{w})$，$\boldsymbol{w} \in GF^n(2)$ 是其Walsh循环谱，记

$$\boldsymbol{S}_{f0} = \{\boldsymbol{w}:\boldsymbol{w} \in GF^n(2), S_{(f)}(\boldsymbol{w}) = 0\},$$

则 $f(\boldsymbol{x})$，$\boldsymbol{x} \in GF^n(2)$ 线性等价于某 $m$ 阶相关免疫的布尔函数的充分必要条件是存在GF(2)上的 $n \times n$ 可逆矩阵 $\boldsymbol{B}$ 及 $\boldsymbol{b} \in GF^n(2)$，使得

$$(\boldsymbol{w}(i_1, \cdots, i_k) + \boldsymbol{b})\boldsymbol{B} \in \boldsymbol{S}_{f0},$$

$$1 \leqslant i_1 < \cdots < i_k \leqslant n, 1 \leqslant k \leqslant m。$$

证明　以 $\boldsymbol{B}$ 取代式(4)中的 $(\boldsymbol{A}^{-1})^{\mathrm{T}}$，根据Xiao-massey定理即得。

定理4　设 $f(\boldsymbol{x})$，$\boldsymbol{x} \in GF^n(2)$ 是 $n$ 元布尔函数，$S_{(f)}(\boldsymbol{w})$，$\boldsymbol{w} \in GF^n(2)$ 是其Walsh循环谱，记

$$\boldsymbol{S}_{f0} = \{\boldsymbol{w}:\boldsymbol{w} \in GF^n(2), S_{(f)}(\boldsymbol{w}) = 0\},$$

那么，若 $\boldsymbol{S}_{f0}$ 中存在 $n$ 个线性无关的向量 $\boldsymbol{v}^{(1)}$，…，$\boldsymbol{v}^{(n)}$，且

$$\boldsymbol{v}^{(i_1)} + \cdots + \boldsymbol{v}^{(i_k)} \in \boldsymbol{S}_{f0},$$

$$1 \leqslant i_1 < \cdots < i_k \leqslant n, 1 \leqslant k \leqslant m,$$

则 $f(\boldsymbol{x})$，$\boldsymbol{x} \in GF^n(2)$ 线性等价于具有 $m$ 阶相关免疫性的布尔函数

$$g(\boldsymbol{x}) = f(\boldsymbol{x}\boldsymbol{A}+\boldsymbol{a}) + c,\ \boldsymbol{x} \in GF^n(2),$$

其中 $\boldsymbol{A}$ 是GF(2)上的 $n \times n$ 可逆矩阵，使得 $(\boldsymbol{A}^{-1})^{\mathrm{T}}$ 正是以 $\boldsymbol{S}_{f0}$ 中上述 $\boldsymbol{v}^{(1)}$，…，$\boldsymbol{v}^{(n)}$ 为行所得到的矩阵，而 $\boldsymbol{a} \in GF^n(2)$ 和 $c \in GF(2)$ 任意取定。

证明　在定理3中取 $\boldsymbol{b} = 0 \in GF^n(2)$ 即得。

注：文献[4]中所提到的LT方法的理论本质上就是定理4中的 $m=1$ 的情况。

再以 $\boldsymbol{s}(i) \in GF^n(2)$ 表示只有第 $i$ 个分量取值为1的 $n$ 维布尔向量，$1 \leqslant i \leqslant n$，…。一般地，以 $\boldsymbol{s}(i_1, \cdots, i_k) \in GF^n(2)$ 表示只有第 $i_1$ 个分量、……、第 $i_k$ 个分量取值为1的 $n$ 维布尔向量，$1 \leqslant i_1 < \cdots < i_k \leqslant n$，$1 \leqslant k \leqslant n-1$，则有

定理5　设 $f(\boldsymbol{x})$，$\boldsymbol{x} \in GF^n(2)$ 是 $n$ 元布尔函数，$r_f(\boldsymbol{s})$，$\boldsymbol{s} \in GF^n(2)$ 是其自相关函数，记

$$\boldsymbol{R}_{f0} = \{\boldsymbol{s}:\boldsymbol{s} \in GF^n(2), r_f(\boldsymbol{s}) = 0\},$$

则 $f(\boldsymbol{x}),\boldsymbol{x}\in \mathrm{GF}^n(2)$ 线性等价于某满足 $k$ 次扩散准则的布尔函数的充分必要条件是 $\boldsymbol{R}_{f0}$ 中存在 $n$ 个线性无关的向量 $\tau^{(1)},\cdots,\tau^{(n)}$，且

$$\tau^{(i_1)}+\cdots+\tau^{(i_h)}\in \boldsymbol{R}_{f0},$$
$$1\leqslant i_1<\cdots<i_h\leqslant n,1\leqslant h\leqslant k。$$

证明　首先考虑 $k=1$ 的情况：

必要性　设与 $f(\boldsymbol{x}),\boldsymbol{x}\in \mathrm{GF}^n(2)$ 线性等价的 $g(\boldsymbol{x})=f(\boldsymbol{xA}+\boldsymbol{a})+\boldsymbol{b}\cdot\boldsymbol{x}+c$ 满足严格雪崩准则，即有 $r_g(\boldsymbol{s}(i))=0,1\leqslant i\leqslant n$，记矩阵 $\boldsymbol{A}$ 的第 $i$ 行为 $\boldsymbol{\tau}^{(i)},1\leqslant i\leqslant n$，而根据式（3）知

$$r_f(\boldsymbol{s}(i)\boldsymbol{A})=r_g(\boldsymbol{s}(i))=0,\quad 1\leqslant i\leqslant n,$$

就是说

$$\tau^{(i)}=\boldsymbol{s}(i)\boldsymbol{A}\in \boldsymbol{R}_{f0},1\leqslant i\leqslant n,$$

且由矩阵 $\boldsymbol{A}$ 可逆还知 $\tau^{(i)},1\leqslant i\leqslant n$ 线性无关。

充分性　若 $\boldsymbol{R}_{f0}$ 中存在 $n$ 个线性无关的向量 $\tau^{(1)},\cdots,\tau^{(n)}$，记以 $\tau^{(1)},\cdots,\tau^{(n)}$ 为行的矩阵为 $\boldsymbol{A}$，则对任意的 $\boldsymbol{a},\boldsymbol{b}\in \mathrm{GF}^n(2)$ 及 $c\in \mathrm{GF}(2)$，根据式(3) 知与 $f(\boldsymbol{x})$ 线性等价的

$$g(\boldsymbol{x})=f(\boldsymbol{xA}+\boldsymbol{a})+\boldsymbol{b}\cdot\boldsymbol{x}+c$$

的自相关函数都满足

$$r_g(\boldsymbol{s}(i))=(-1)^{\boldsymbol{b}\cdot\boldsymbol{s}(i)}r_f(\boldsymbol{s}(i)\boldsymbol{A})=(-1)^{\boldsymbol{b}\cdot\boldsymbol{s}(i)}r_f(\boldsymbol{\tau}^{(i)}),1\leqslant i\leqslant n,$$

可见 $g(\boldsymbol{x})=f(\boldsymbol{xA}+\boldsymbol{a})+\boldsymbol{b}\cdot\boldsymbol{x}+c$ 都满足严格雪崩准则。

又注意到

$$\boldsymbol{s}(i_1,\cdots,i_h)=\boldsymbol{s}(i_1)+\cdots+\boldsymbol{s}(i_h),1\leqslant h\leqslant k,$$

同理可知定理 5 成立。

注：显然，综合定理 3 或定理 4 与定理 5 的条件，即可得到一个布尔函数线性等价于一个既具有某阶相关免疫性、也满足某次扩散准则的布尔函数的条件，也同时提供了一种构造既具有相关免疫性、也满足扩散准则的布尔函数的方法。

例 1　设 5 元布尔函数

$$f(x_1,x_2,x_3,x_4,x_5)=x_1x_2x_3+x_2x_3x_4+x_1x_2+x_1x_3+x_1x_4+x_1x_5+x_2x_5+x_3x_4+x_4x_5+x_1+x_2,$$

其中 $(x_1,x_2,x_3,x_4,x_5)\in \mathrm{GF}^5(2)$。算得

$\boldsymbol{S}_{f0}=\{(0,0,0,0,0),(0,0,0,0,1),(0,0,0,1,0),(0,0,1,0,0),(1,0,0,0,0),(1,1,0,0,0),(1,0,1,0,0),(0,0,1,0,1),(0,0,1,1,0),(0,1,0,0,1),(0,1,0,1,0),(0,1,1,0,0),(1,1,1,0,0),(1,1,0,1,0),(0,1,1,1,0),(1,0,0,1,1),(1,0,1,1,0),(1,1,1,1,0),(1,1,0,1,1),(1,0,1,1,1),(1,1,1,1,1)\}$，

$\boldsymbol{R}_{f0}=\{(0,0,0,0,1),(0,0,0,1,0),(0,1,0,0,0),(1,0,0,0,0),(0,0,0,1,1),(0,1,0,0,1),(0,0,1,1,0),(0,1,1,0,0),(1,0,0,0,1),(1,0,0,1,0),(1,0,1,0,0),(0,0,1,1,1),(0,1,1,0,1),(1,0,1,0,1),(1,1,0,1,0),(1,1,0,1,1),(1,1,1,1,0),(1,1,1,1,1)\}$，

易知 $f$ 平衡。因为 $(0,1,0,0,0)\notin \boldsymbol{S}_{f0}$，$(0,0,1,0,0)\notin \boldsymbol{R}_{f0}$，所以由定义 2 和引理 3 还知 $f$ 不具有相关免疫性且不满足 SAC。在 $\boldsymbol{S}_{f0}$ 中取 5 个线性无关的向量构成矩阵 $(\boldsymbol{A}^{-1})^{\mathrm{T}}$：

$$(\boldsymbol{A}^{-1})^{\mathrm{T}}=\begin{pmatrix}1&0&0&0&0\\0&1&1&0&0\\0&0&1&0&0\\0&0&0&1&0\\0&0&0&0&1\end{pmatrix},$$

得

$$A=\begin{pmatrix}1&0&0&0&0\\0&1&0&0&0\\0&1&1&0&0\\0&0&0&1&0\\0&0&0&0&1\end{pmatrix}。$$

由于 $\boldsymbol{A}$ 的 5 个行向量正好都在 $\boldsymbol{R}_{f0}$ 中，所以根据可逆线性变换的不变性及定理 4 和定理 5 知，与 $f$ 线性等价的布尔函数

$$g(\boldsymbol{x})=f(\boldsymbol{xA}+\boldsymbol{a})+c,\boldsymbol{x}\in \mathrm{GF}^5(2)$$

平衡、具有相关免疫性并且满足 SAC，其中 $\boldsymbol{a}\in \mathrm{GF}^5(2)$ 和 $c\in \mathrm{GF}(2)$ 任意取定。如取

$$(0,0,0,0,0)=0=\boldsymbol{a},c=0,$$

则布尔函数

$$g(\boldsymbol{x})=f(\boldsymbol{xA})=f(x_1,x_2+x_3,x_3,x_4,x_5)=(x_1+x_2+x_3+x_4)x_5+x_1+x_2+x_3+x_1x_2+x_1x_3+x_1x_4+x_1x_2x_3+x_2x_3x_4=x_1x_2x_3+x_2x_3x_4+x_1x_2+x_1x_3+x_1x_4+x_1x_5+x_2x_5+x_3x_5+x_4x_5+x_1+x_2+x_3$$

平衡、具有相关免疫性且满足 SAC，而直接由定义容易验证 $g(\boldsymbol{x})$ 确实是平衡、具有相关免疫性且满足 SAC 的。

例 2　设 5 元布尔函数

$$f(x_1,x_2,x_3,x_4,x_5)=x_1x_2+x_3x_4+x_5,$$

$$(x_1, x_2, x_3, x_4, x_5) \in \mathrm{GF}^5(2),$$

得到

$$\boldsymbol{S}_{f0} = \{(w_1, w_2, w_3, w_4, 0) : (w_1, w_2, w_3, w_4) \in \mathrm{GF}^4(2)\},$$

$$\boldsymbol{R}_{f0} = \mathrm{GF}^5(2) \setminus \{(0,0,0,0,0), (0,0,0,0,1)\},$$

因为 $(0,0,0,0,1) \notin \boldsymbol{S}_{f0}$, $(0,0,0,0,1) \notin \boldsymbol{R}_{f0}$, 由定义2和引理3知 $f$ 不具有相关免疫性且不满足SAC。取可逆矩阵

$$(\boldsymbol{A}^{-1})^{\mathrm{T}} = B = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix},$$

得

$$\boldsymbol{A} = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix},$$

又取 $\boldsymbol{b} = (0,0,0,0,1)$, 因为 $(\boldsymbol{w}(i) + \boldsymbol{b})\boldsymbol{B} \in \boldsymbol{S}_{f0}$, $1 \leqslant i \leqslant 5$, 且 $\boldsymbol{A}$ 的5个行向量正好都在 $\boldsymbol{R}_{f0}$ 中, 所以根据定理3和定理5知, 与 $f$ 线性等价的布尔函数

$$g(\boldsymbol{x}) = f(\boldsymbol{xA} + \boldsymbol{a}) + \boldsymbol{b} \cdot \boldsymbol{x} + c, \boldsymbol{x} \in \mathrm{GF}^5(2),$$

具有相关免疫性且满足SAC, 其中 $\boldsymbol{a} \in \mathrm{GF}^5(2)$ 和 $c \in \mathrm{GF}(2)$ 任意取定。如取

$$(0,0,0,0,0) = 0 = \boldsymbol{a}, c = 0,$$

则布尔函数

$$g(\boldsymbol{x}) = f(\boldsymbol{xA}) + \boldsymbol{b} \cdot \boldsymbol{x} = f(x_2 + x_5, x_1 + x_5, x_1 + x_2 + x_3 + x_5, x_1 + x_2 + x_4 + x_5, x_1 + x_2 + x_5) + x_5 = (x_2 + x5)(x_1 + x_5) + (x_1 + x_2 + x_3 + x_5)(x_1 + x_2 + x_4 + x_5) + (x_1 + x_2 + x_5) + x_5 = x_1x_2 + x_1x_3 + x_1x_4 + x_1x_5 + x_2x_3 + x_2x_4 + x_2x_5 + x_3x_4 + x_3x_5 + x_4x_5$$

具有相关免疫性且满足SAC, 而直接由定义容易验证 $g(\boldsymbol{x})$ 确实是具有相关免疫性且满足SAC的。

不难知, 在例1和例2中还能构造别的与题设5元布尔函数 $f$ 线性等价的、既具有相关免疫性也满足SAC的布尔函数。

## 4 结语

笔者利用概率方法得到了线性等价的2个布尔函数的Walsh循环谱及自相关函数之间的关系, 由此给出了一个布尔函数线性等价于 $m$ 阶相关免疫函数的Walsh循环谱刻画和线性等价于 $k$ 次扩散准则函数的自相关刻画, 并给出了利用线性等价性构造同时具有相关免疫性和扩散性的布尔函数的方法和实例, 为在密码设计中将某些不满足相关免疫要求和扩散要求(但满足适定条件)的布尔函数线性变换为满足要求的函数提供了一种方法, 同时也为设计密钥流非线性组合生成器时综合各种优良性的需求提供了可行性。

致谢: 感谢郭锦辉先生对论文工作的帮助!

### 参考文献

[1] Zheng Y, Pieprzyk J, Seberry J. Haval-one-way hashing algorithm with variable length of output [A]. Advances in Cryptology-AUSCRYPT'92, Vol 718, Lecture Notes in Computer Science [C]. Springer-Verlag, Berlin, Heidelberg, New York, 1993. 83~104

[2] Seberry J, Zhang Xianmo, Zheng Yuliang. Nonlinearity and propagation characteristics of balanced Boolean functions [A]. Advances in Cryptology-CRYPTO'93 [C]. Springer-Verlag, 1994. 49~60

[3] Pasalic E, Johansson T. Further results on the relation between nonlinearity and resiliency of Boolean functions [A]. Proc IMA Conf Cryptography and Coding (Lecture Notes in Computer Science) Vol 1746 [C]. New York: Springer-Verlag, 1999. 35~45

[4] Maitra S, Pasalic E. Further construction of resilient Boolean functions with very high nonlinearity [J]. IEEE Trans, On Information Theory, 2002, 48(7): 1825~1834, 234, 235, 243

[5] 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. 8

[6] 李世取, 曾本胜, 廉玉忠, 等. 密码学中的逻辑函数 [M]. 北京: 中软电子出版社, 2003

[7] 冯登国, 裴定一. 密码学导引 [M]. 北京: 科学出版社, 1999

[8] 李世取, 曾本胜. 概率方法在布尔函数相关免疫性研究中的应用 [J]. 数理统计与应用概率, 1994, (1): 5~9

[9] 肖国镇, Massey. A spectral characterization of correlation-immune function [J]. IEEE Trans, 1988, (IT-34): 569~571

[10] Chee S, Lee S, Kim K. Semi-bent functions [A]. Advances in Cryptology ASIACRYPT'94 [C]. Springer, 1995. 107~118

# The Characteristic of Spectrum and Self-correlation of Some Boolean Fuctions Linearly Equivalent to Specific Cryptographic Functions

Yang Rui, Zeng Bensheng, Li Shiqu

(*Department of Information Research, PLA Information Engineering College, Zhengzhou* 450002, *China*)

[**Abstract**] The paper made an analysis of the similarities and differences about the cryptographic properties of two Boolean functions in the sense of linearly equivalence, and obtained a sufficient and necessary condition about a Boolean function linearly equivalent to some $m$ order correlation-immune Boolean function. It also obtained a sufficient and necessary condition about a Boolean function linearly equivalent to some Boolean function satisfying the $k$ order propagation criterion. Moreover, it showed an example, in which a given Boolean function, that is not correlation-immuned and does not satisfy the propagation criterion can be constructed into a correlation-immuned Boolean function that can satisfy the propagation criterion and is linearly equivalent to the former one.

[**Key words**] linear equivalence; Walsh cycle spectrum; self-correlation function; correlation-immunity; propagation criterion; SAC

(cont. from p.59)

# The Study of Sprinkler Performance in Fire

Zhang Cunfeng, Huo Ran, Li Yuanzhou

(*The state key laboratory of fire science, USTC, Hefei* 230027, *China*)

[**Abstract**] This paper studied on the activation time of sprinkler and the critical heat release rate to activate the sprinkler when a fire happened. By calculation, this paper gave the curve on the activation time and the factors which would impact the activation time. The following conclusions were done: the activation time was almost linear with the installation height and the environment temperature; the fire development mode would affect the increasing rate of the activation time; the exponential relationship was found between the activation time and the response time index (RTI). As the height increased, the critical heat release rate would increase. In order to control fire effectively, the fast response sprinkler must be used when the sprinkler was installed in a high building ceiling.

[**Key words**] sprinkler head; critical heat release rate; response time