m 值“复合”逻辑函数的 Chrestenson 循环谱、自相关函数及应用

李迎东 李世取
(解放军信息工程学院 信息研究系 郑州 450002)

摘 要 该文利用反演公式求得了 *m* 值“复合”逻辑函数的 Chrestenson 循环谱的计算公式，并由此得到了 *m* 值“复合”逻辑函数的自相关函数的计算公式，进而运用这两个公式，给出了 *m* 值“复合”逻辑函数具备平衡性、相关免疫性的条件，并对 *m* 值“复合”逻辑函数的自相关函数及其性质进行了分析；此外该文还得到有限个 *m* 值“复合”逻辑函数的非零线性和函数的 Chrestenson 循环谱的计算公式。

关键词 反演公式, Chrestenson 循环谱，自相关函数，平衡，相关免疫
中图分类号:：TN918.1 **文献标识码**：A **文章编号**：1009-5896(2006)07-1258-04

Chrestenson Spectrum and Auto-correlation Function of *m*-value “Composition” Logical Function and Applications

Li Ying-dong Li Shi-qu
(*Department of Information Research, PLA Information Engineering College, Zhengzhou* 450002, *China*)

Abstract This paper presents the formula of Chrestenson spectrum of m-value “composition” logical function by using inversion formula, and gives the formula of auto-correlation function of *m*-value “composition” logical function. Furthermore, this paper gives some conditions under which *m*-value “composition” logical function is separate balanced or correlation-immune, and analyzes the auto-correlation function of *m*-value “composition” logical function and its charateristic. Moreover, this paper gets the Chrestenson spectrum formular of nonzero linear combination of several *m*-value “composition” logical functions.

Key words Inversion formula, Chrestenson spectrum, Auto-correlation, Balance, Correlation-immune

1 引言

非线性组合生成器是序列密码中经常使用的一类重要的密钥流生成器，它是由一组线性移位寄存器(LFSR)通过一个非线性组合函数 f 组合而成的生成器，其密码学性能常取决于所选组合函数的性质(见文献[1])。为了提高密码体制的安全强度，密码设计者在非线性组合生成器的基础上，又提出了对多个非线性组合生成器的输出序列再进行多层次非线性组合的密钥流生成器，这里就用到了“复合”逻辑函数 $G(f_1,\cdots,f_k)$。文献[2,3]在二元域上对布尔“复合函数”已做过一些研究，得到了布尔“复合函数”的Walsh循环谱计算公式。文献[3]还得到了布尔“复合函数”的自相关函数计算公式，目前关于 *m* 值“复合”逻辑函数的其他研究成果在国内尚未见到。

由于实际应用的需求和学科自身发展的规律使然，近年来人们在密码学中对多值逻辑函数的有关性质和应用研究给予了较多的关注。同布尔函数的情形类似，多值逻辑函数的一些密码学性质，如平衡性，抗最佳仿射逼近性能，相关免疫性，扩散性等也都能用其Chrestenson循环谱及自相关函数予以刻画[4]。故 *m* 值逻辑函数的Chrestenson循环谱及其自相关函数在 *m* 值逻辑函数的性质研究中仍发挥重要作用。因此我们利用反演公式求得了 *m* 值“复合”逻辑函数的Chrestenson循环谱计算公式。这一算式与布尔“复合函数”的Walsh循环谱计算公式实质上是完全一致的。运用这一公式我们给出了“复合”逻辑函数具备平衡性、相关免疫性等密码学性质的条件。利用 *m* 值逻辑函数的Chrestenson循环谱，我们进一步求得了 *m* 值“复合”逻辑函数的自相关函数计算公式。这一算式与布尔“复合函数”自相关函数计算公式在本质上也是一致的。应用这一公式我们对 *m* 值“复合”逻辑函数的自相关性质进行了分析。此外我们还利用 *m* 值“复合”逻辑函数的Chrestenson循环谱，给出了有限个 *m* 值“复合”逻辑函数的非零线性和函数的Chrestenson循环谱计算公式。它在分析 *m* 值“复合”向量逻辑函数的有关密码学性质时将会发挥重要作用。

2 预备知识

以下不加说明 $k\ge 2, n\ge 2$ 是整数。

定义 1 设 $\boldsymbol{f}^{(k)}(\boldsymbol{x})=(f_1(\boldsymbol{x}),\cdots,f_k(\boldsymbol{x}))$，$\boldsymbol{x}=(x_1,\cdots,x_n)\in Z_m^n$ 是任意 k 维 *m* 值向量逻辑函数，而

$$G(z_1,\cdots,z_k),\qquad \boldsymbol{z}=(z_1,\cdots,z_k)\in Z_m^k$$

是任一 k 元 *m* 值逻辑函数，称 n 元 *m* 值逻辑函数：

$$G\big(f_1(\boldsymbol{x}),\cdots,f_k(\boldsymbol{x})\big),\qquad \boldsymbol{x}\in Z_m^n$$

为 k 元 *m* 值逻辑 $G(\boldsymbol{z})$ 和 k 维 *m* 值向量逻辑函数 $\boldsymbol{f}^{(k)}(\boldsymbol{x})$ 的 *m* 值“复合”逻辑函数，以下简称“复合函数”。

2004-12-16 收到，2005-07-11 改回
计算机网络与信息安全教育部重点实验室资助课题

定义 2[5]　设 $\boldsymbol{x}=(x_1,\cdots,x_n)\in Z_m^n$, $\boldsymbol{w}=(w_1,\cdots,w_n)\in Z_m^n$, $\boldsymbol{x}$ 和 $\boldsymbol{w}$ 的点积为

$$\boldsymbol{w}\cdot\boldsymbol{x}=w_1x_1+\cdots+w_nx_n(\mathrm{mod}\,m)$$

n 元 m 值逻辑函数 $f(\boldsymbol{x})$, $\boldsymbol{x}\in Z_m^n$ 的第二种 Chrestenson 变换定义为

$$S_{(f)}(\boldsymbol{w})=\frac{1}{m^n}\sum_{\boldsymbol{x}\in Z_m^n}u^{f(\boldsymbol{x})-\boldsymbol{w}\boldsymbol{x}},\quad \boldsymbol{w}\in Z_m^n$$

称 $S_{(f)}(\boldsymbol{w})$, $\boldsymbol{w}\in Z_m^n$ 为 $f(\boldsymbol{x})$ 的第二种 Chrestenson 谱, 也称之为 Chrestenson 循环谱。

定义 3[4]　设 $f(\boldsymbol{x})$, $\boldsymbol{x}\in Z_m^n$ 是 m 值逻辑函数, 对

$$\boldsymbol{x}=(x_1,x_2,\cdots,x_n)\in Z_m^n,\quad \boldsymbol{s}=(s_1,s_2,\cdots,s_n)\in Z_m^n$$

记 $\boldsymbol{x}+\boldsymbol{s}=(x_1+s_1,x_2+s_2,\cdots,x_n+s_n)$, 称

$$r_f(\boldsymbol{s})=\frac{1}{m^n}\sum_{\boldsymbol{x}\in Z_m^n}u^{f(\boldsymbol{x}+\boldsymbol{s})-f(\boldsymbol{x})},\quad \boldsymbol{s}\in Z_m^n$$

为 m 值逻辑函数 $f(\boldsymbol{x})$, $\boldsymbol{x}\in Z_m^n$ 的自相关函数。

又设 $g(\boldsymbol{x}),\boldsymbol{x}\in Z_m^n$ 是 m 值逻辑函数, 称

$$r_{f,g}(\boldsymbol{s})=\frac{1}{m^n}\sum_{\boldsymbol{x}\in Z_m^n}u^{f(\boldsymbol{x}+\boldsymbol{s})-g(\boldsymbol{x})},\quad \boldsymbol{s}\in Z_m^n$$

为 m 值逻辑函数 $f(\boldsymbol{x})$ 和 $g(\boldsymbol{x})$ 的互相关函数。

定义 4[4]　广义Bent函数的等价定义 设 $f(\boldsymbol{x}),\boldsymbol{x}\in Z_m^n$ 是 m 值逻辑函数, 若对任意 $\boldsymbol{w}\in Z_m^n$, 都有

$$\left|S_{(f)}(\boldsymbol{w})\right|=\frac{1}{m^{n/2}}$$

则称 $f(\boldsymbol{x})$ 为广义 Bent 函数。

引理 1[5]　(反演公式)　任一 n 元 m 值逻辑函数 $f(\boldsymbol{x}),\boldsymbol{x}\in Z_m^n$ 与其Chrestenson循环谱的关系如下

$$u^{f(\boldsymbol{x})}=\sum_{\boldsymbol{w}\in Z_m^n}S_{(f)}(\boldsymbol{w})u^{\boldsymbol{w}\cdot\boldsymbol{x}},\quad \boldsymbol{x}\in Z_m^n$$

引理 2[4]　设 $f(\boldsymbol{x}),\boldsymbol{x}\in Z_m^n$ 是 m 值逻辑函数, 其自相关函数和Chrestenson循环谱分别为 $r_f(\boldsymbol{s})$ 和 $S_{(f)}(\boldsymbol{w})$, 则

$$\sum_{\boldsymbol{w}\in Z_m^n}\left|S_{(f)}(\boldsymbol{w})\right|^2u^{\boldsymbol{w}\cdot\boldsymbol{s}}=r_f(\boldsymbol{s}),\quad \boldsymbol{s}\in Z_m^n$$

又设 $f_1(\boldsymbol{x}),f_2(\boldsymbol{x}),\boldsymbol{x}\in Z_m^n$ 是两个 m 值逻辑函数, 其互相关函数为 $r_{f_1,f_2}(\boldsymbol{s})$, 则

$$\sum_{\boldsymbol{w}\in Z_m^n}S_{(f_1)}(\boldsymbol{w})\cdot\overline{S_{(f_2)}(\boldsymbol{w})}u^{\boldsymbol{w}\cdot\boldsymbol{s}}=r_{f_1,f_2}(\boldsymbol{s}),\quad \boldsymbol{s}\in Z_m^n$$

引理 3[4]　k 维 m 值向量逻辑函数 $\boldsymbol{f}^{(k)}(\boldsymbol{x})=\left(f_1(\boldsymbol{x}),\cdots,f_k(\boldsymbol{x})\right)$, $\boldsymbol{x}=(x_1,\cdots,x_n)\in Z_m^n$ 是 t 阶相关免疫的充要条件是对任意的 $\boldsymbol{w}\in Z_m^n$, 其汉明重量 $1\le W(\boldsymbol{w})\le t$ 时, 都有

$$S_{(v_1f_1+\cdots+v_kf_k)}(\boldsymbol{w})=0,\quad (v_1,\cdots,v_k)\in Z_m^k\setminus\{\boldsymbol{0}\}$$

引理 4[4]　m 值逻辑函数 $f(\boldsymbol{x}),\boldsymbol{x}=(x_1,\cdots,x_n)\in Z_m^n$ 为 t 阶相关免疫的充要条件是对任意的 $\boldsymbol{w}\in Z_m^n$, 其汉明重量 $1\le W(\boldsymbol{w})\le t$ 时, 都有

$$S_{(\lambda f)}(\boldsymbol{w})=0,\quad \lambda\in Z_m\setminus\{0\}$$

3　主要结论

由于 m 值逻辑函数的许多密码学性质也可以通过其 Chrestenson 谱予以刻画, 故 m 值逻辑函数的 Chrestenson 循环谱在 m 值逻辑函数的性质研究中仍能发挥重要作用。冯登国教授在文献[1]中就此进行过专门研究。下面我们给出“复合函数”的 Chrestenson 循环谱计算公式:

定理 1　设 $\boldsymbol{f}^{(k)}(\boldsymbol{x})=\left(f_1(\boldsymbol{x}),\cdots,f_k(\boldsymbol{x})\right)$, $\boldsymbol{x}=(x_1,\cdots,x_n)\in Z_m^n$ 是任意 k 维 m 值向量逻辑函数, 而 $G(z_1,\cdots,z_k)$, $(z_1,\cdots,z_k)\in Z_m^k$ 是任一 k 元 m 值逻辑函数, 则 n 元“复合函数” $G\left(f_1(\boldsymbol{x}),f_k(\boldsymbol{x})\right)$, $\boldsymbol{x}\in Z_m^n$ 的 Chrestenson 谱为

$$S_{(G(f_1,\cdots,f_k))}(\boldsymbol{w})=\sum_{\boldsymbol{v}=(v_1,\cdots,v_k)\in Z_m^k}S_{(G)}(\boldsymbol{v})S_{(v_1f_1+\cdots+v_kf_k)}(\boldsymbol{w}),\quad \boldsymbol{w}\in Z_m^n \tag{1}$$

特别, 在 $\boldsymbol{w}\in Z_m^n$, $\boldsymbol{w}=\boldsymbol{0}$ 时, 成立

$$S_{(G(f_1,\cdots,f_k))}(\boldsymbol{0})=S_{(G)}(\boldsymbol{0})+\sum_{\boldsymbol{v}=(v_1,\cdots,v_k)\in Z_m^k\setminus\{\boldsymbol{0}\}}S_{(G)}(\boldsymbol{v})S_{(v_1f_1+\cdots+v_kf_k)}(\boldsymbol{0}) \tag{2}$$

在 $\boldsymbol{w}\in Z_m^n$, $\boldsymbol{w}\ne\boldsymbol{0}$ 时, 成立

$$S_{(G(f_1,\cdots,f_k))}(\boldsymbol{w})=\sum_{\boldsymbol{v}=(v_1,\cdots,v_k)\in Z_m^k\setminus\{\boldsymbol{0}\}}S_{(G)}(\boldsymbol{v})S_{(v_1f_1+\cdots+v_kf_k)}(\boldsymbol{w}) \tag{3}$$

证明　因为对任意取定的 $(y_1,\cdots,y_k)\in Z_m^k$, 利用引理 1 有

$$u^{G(y_1,\cdots,y_k)}=\sum_{(v_1,\cdots,v_k)\in Z_m^k}S_{(G)}(v_1,\cdots,v_k)u^{v_1y_1+\cdots+v_ky_k} \tag{4}$$

再注意到对任意取定的 $\boldsymbol{x}\in Z_m^n$, 都有 $\boldsymbol{f}^{(k)}(\boldsymbol{x})=\left(f_1(\boldsymbol{x}),\cdots,f_k(\boldsymbol{x})\right)\in Z_m^k$, 根据式(4)即知

$$u^{G(f_1(\boldsymbol{x}),\cdots,f_k(\boldsymbol{x}))}=\sum_{\boldsymbol{v}=(v_1,\cdots,v_k)\in Z_m^k}S_{(G)}(\boldsymbol{v})\cdot u^{v_1f_1(\boldsymbol{x})+\cdots+v_kf_k(\boldsymbol{x})} \tag{5}$$

由式(5)及 n 元 m 值逻辑函数 $f(\boldsymbol{x})$ 的 Chrestenson 循环谱的定义, 就有

$$\begin{aligned}S_{(G(f_1,\cdots,f_k))}(\boldsymbol{w})&=\frac{1}{m^n}\sum_{\boldsymbol{x}\in Z_m^n}u^{G(f_1(\boldsymbol{x}),\cdots,f_k(\boldsymbol{x}))-\boldsymbol{w}\boldsymbol{x}}\\&=\frac{1}{m^n}\sum_{\boldsymbol{x}\in Z_m^n}u^{G(f_1(\boldsymbol{x}),\cdots,f_k(\boldsymbol{x}))}u^{-\boldsymbol{w}\boldsymbol{x}}\\&=\frac{1}{m^n}\sum_{\boldsymbol{x}\in Z_m^n}\left[\sum_{\boldsymbol{v}=(v_1,\cdots,v_k)\in Z_m^k}S_{(G)}(\boldsymbol{v})\,u^{v_1f_1(\boldsymbol{x})+\cdots+v_kf_k(\boldsymbol{x})}\right]u^{-\boldsymbol{w}\boldsymbol{x}}\\&=\sum_{\boldsymbol{v}=(v_1,\cdots,v_k)\in Z_m^k}S_{(G)}(\boldsymbol{v})\left[\frac{1}{m^n}\sum_{\boldsymbol{x}\in Z_m^n}u^{v_1f_1(\boldsymbol{x})+\cdots+v_kf_k(\boldsymbol{x})-\boldsymbol{w}\boldsymbol{x}}\right]\\&=\sum_{\boldsymbol{v}=(v_1,\cdots,v_k)\in Z_m^k}S_{(G)}(\boldsymbol{v})\cdot S_{(v_1f_1+\cdots+v_kf_k)}(\boldsymbol{w}),\quad \boldsymbol{w}\in Z_m^n\end{aligned}$$

又因为 $S_{(0)}(\boldsymbol{w})=\frac{1}{m^n}\sum_{\boldsymbol{x}\in Z_m^n}u^{-\boldsymbol{w}\boldsymbol{x}}=\begin{cases}0, & \boldsymbol{w}\ne\boldsymbol{0},\\ 1, & \boldsymbol{w}=\boldsymbol{0},\end{cases}$ 从而就有在 $\boldsymbol{w}\in Z_m^n$, $\boldsymbol{w}=\boldsymbol{0}$ 时,

$$S_{(G(f_1,\cdots,f_k))}(\boldsymbol{0})=S_{(G)}(\boldsymbol{0})+\sum_{\boldsymbol{v}=(v_1,\cdots,v_k)\in Z_m^k\setminus\{\boldsymbol{0}\}}S_{(G)}(\boldsymbol{v})\cdot S_{(v_1f_1+\cdots+v_kf_k)}(\boldsymbol{0})$$

成立; 在 $\boldsymbol{w}\in Z_m^n$, $\boldsymbol{w}\neq\boldsymbol{0}$ 时,

$$S_{(G(f_1,\cdots,f_k))}(\boldsymbol{w})=\sum_{\boldsymbol{v}=(v_1,\cdots,v_k)\in Z_m^k\setminus\{\boldsymbol{0}\}} S_{(G)}(\boldsymbol{v})\cdot S_{(v_1f_1+\cdots+v_kf_k)}(\boldsymbol{w})$$ 成立。

证毕

注 1 特别在 $m=2$ 时, 定理 1 的结论即是文献[2,3]中得到的布尔“复合函数”的 Walsh 循环谱的计算公式。

由定理 1, 我们还容易得到有限个“复合函数”非零线性和函数的 Chrestenson 循环谱计算公式, 即推论 1。

推论 1 设 $l\geq 1$, $\boldsymbol{f}^{(k)}(\boldsymbol{x})=(f_1(\boldsymbol{x}),\cdots,f_k(\boldsymbol{x})),\boldsymbol{x}\in Z_m^n$ 是 k 维 n 元 m 值向量逻辑函数, 而

$$\boldsymbol{G}^{(l)}(\boldsymbol{z})=\big(G_1(\boldsymbol{z}),\cdots,G_l(\boldsymbol{z})\big),\quad \boldsymbol{z}\in Z_m^k$$

是 l 维 k 元 m 值向量逻辑函数, 记 l 维 n 元 m 值“复合”向量逻辑函数:

$$\boldsymbol{G}^{(l)}\big(f_1(\boldsymbol{x}),\cdots,f_k(\boldsymbol{x})\big)=\big(G_1\big(f_1(\boldsymbol{x}),\cdots,f_k(\boldsymbol{x})\big),\cdots,G_l\big(f_1(\boldsymbol{x}),\cdots,f_k(\boldsymbol{x})\big)\big),\quad \boldsymbol{x}\in Z_m^n$$

则对任意的 $\boldsymbol{w}\in Z_m^n$ 以及 $\boldsymbol{0}\neq\boldsymbol{\lambda}=(\lambda_1,\cdots,\lambda_l)\in Z_m^l$, 都有

$$S_{(\boldsymbol{\lambda}\boldsymbol{G}^{(l)}(f_1,\cdots,f_k))}(\boldsymbol{w})=\sum_{\boldsymbol{v}=(v_1,\cdots,v_k)\in Z_m^k} S_{(v_1f_1+\cdots+v_kf_k)}(\boldsymbol{w})\cdot S_{(\lambda_1G_1+\cdots+\lambda_lG_l)}(\boldsymbol{v})$$

证明 注意到对任给的 $\boldsymbol{0}\neq\boldsymbol{\lambda}=(\lambda_1,\cdots,\lambda_l)\in Z_m^l$,

$$\begin{aligned}&\lambda_1G_1(f_1(\boldsymbol{x}),\cdots,f_k(\boldsymbol{x}))+\cdots+\lambda_lG_l(f_1(\boldsymbol{x}),\cdots,f_k(\boldsymbol{x}))\\&\quad=(\lambda_1G_1+\cdots+\lambda_lG_l)\big(f_1(\boldsymbol{x}),\cdots,f_k(\boldsymbol{x})\big)\end{aligned}$$

对任意的 $\boldsymbol{w}\in Z_m^n$, 在定理 1 中特别取

$$G(\boldsymbol{z})=\lambda_1G_1(\boldsymbol{z})+\cdots+\lambda_lG_l(\boldsymbol{z}),\quad \boldsymbol{z}\in Z_m^k$$

由定理 1 中的式(1)即得欲证式。 证毕

m 值逻辑函数的自相关函数是定义在 Z_m^n 上的复值函数, 与布尔函数情况类似, 它也能刻划 m 值逻辑函数的“扩散”特征和“线性结构”特征,下面利用定理 1, 通过 G 的 Chrestenson 循环谱和与 $f_1(\boldsymbol{x}),\cdots,f_k(\boldsymbol{x})$ 有关的 Chrestenson 循环谱及相关函数来得到“复合函数” $G\big(f_1(\boldsymbol{x}),\cdots,f_k(\boldsymbol{x})\big)$ 的自相关函数的计算公式。

定理 2 设 $\boldsymbol{f}^{(k)}(\boldsymbol{x})=\big(f_1(\boldsymbol{x}),\cdots,f_k(\boldsymbol{x})\big)$, $\boldsymbol{x}\in Z_m^n$ 是任意 k 维 m 值向量逻辑函数, 而 $G(\boldsymbol{z})$, $\boldsymbol{z}\in Z_m^k$ 是任一 k 元 m 值逻辑函数, 则“复合函数” $G\big(f_1(\boldsymbol{x}),\cdots,f_k(\boldsymbol{x})\big)$, $\boldsymbol{x}\in Z_m^n$ 的自相关函数为

$$\begin{aligned}&r_{G(f_1,\cdots,f_k)}(\boldsymbol{s})\\&=\big|S_{(G)}(\boldsymbol{0})\big|^2+S_{(G)}(\boldsymbol{0})\sum_{\boldsymbol{0}\neq\boldsymbol{v}=(v_1,\cdots,v_k)\in Z_m^k}\overline{S_{(G)}(\boldsymbol{v})}\,\overline{S_{(v_1f_1+\cdots+v_kf_k)}(\boldsymbol{0})}\\&+\overline{S_{(G)}(\boldsymbol{0})}\sum_{\boldsymbol{0}\neq\boldsymbol{v}=(v_1,\cdots,v_k)\in Z_m^k}S_{(G)}(\boldsymbol{v})S_{(v_1f_1+\cdots+v_kf_k)}(\boldsymbol{0})\\&+\sum_{\boldsymbol{0}\neq\boldsymbol{v}=(v_1,\cdots,v_k)\in Z_m^k}\big|S_{(G)}(\boldsymbol{v})\big|^2r_{\boldsymbol{v}f^{(k)}}(\boldsymbol{s})\\&+\sum_{\substack{\boldsymbol{0}\neq\boldsymbol{v}=(v_1,\cdots,v_k)\in Z_m^k\\ \boldsymbol{v}\neq\boldsymbol{t}=(t_1,\cdots,t_k)\in Z_m^k\setminus\{\boldsymbol{0}\}}}S_{(G)}(\boldsymbol{v})\overline{S_{(G)}(\boldsymbol{t})}\,r_{\boldsymbol{v}f^{(k)},\boldsymbol{t}f^{(k)}}(\boldsymbol{s}),\quad \boldsymbol{s}\in Z_m^n\end{aligned}\tag{6}$$

证明 对任意的 $\boldsymbol{s}\in Z_m^n$, 利用引理 2 及式(2), 式(3), 可得

$$\begin{aligned}&r_{G(f_1,\cdots,f_k)}(\boldsymbol{s})=\sum_{\boldsymbol{w}\in Z_m^k}\big|S_{(G(f_1,\cdots,f_k))}(\boldsymbol{w})\big|^2u^{\boldsymbol{ws}}\\&=\big|S_{(G(f_1,\cdots,f_k))}(\boldsymbol{0})\big|^2+\sum_{\boldsymbol{0}\neq\boldsymbol{w}\in Z_m^k}\big|S_{(G(f_1,\cdots,f_k))}(\boldsymbol{w})\big|^2u^{\boldsymbol{ws}}\\&=\left[S_{(G)}(\boldsymbol{0})+\sum_{\boldsymbol{0}\neq\boldsymbol{v}=(v_1,\cdots,v_k)\in Z_m^k}S_{(G)}(\boldsymbol{v})S_{(v_1f_1+\cdots+v_kf_k)}(\boldsymbol{0})\right]\\&\quad\cdot\left[\overline{S_{(G)}(\boldsymbol{0})}+\sum_{\boldsymbol{0}\neq\boldsymbol{v}=(v_1,\cdots,v_k)\in Z_m^k}\overline{S_{(G)}(\boldsymbol{v})}\,\overline{S_{(v_1f_1+\cdots+v_kf_k)}(\boldsymbol{0})}\right]\\&\quad+\sum_{\boldsymbol{0}\neq\boldsymbol{w}\in Z_m^n}\left[\left[\sum_{\boldsymbol{0}\neq\boldsymbol{v}=(v_1,\cdots,v_k)\in Z_m^k}S_{(G)}(\boldsymbol{v})S_{(v_1f_1+\cdots+v_kf_k)}(\boldsymbol{w})\right]\cdot\sum_{\boldsymbol{0}\neq\boldsymbol{v}=(v_1,\cdots,v_k)\in Z_m^k}\overline{S_{(G)}(\boldsymbol{v})}\,\overline{S_{(v_1f_1+\cdots+v_kf_k)}(\boldsymbol{w})}\right]u^{\boldsymbol{ws}}\right]\\&=\big|S_{(G)}(\boldsymbol{0})\big|^2+S_{(G)}(\boldsymbol{0})\sum_{\boldsymbol{0}\neq\boldsymbol{v}=(v_1,\cdots,v_k)\in Z_m^k}\overline{S_{(G)}(\boldsymbol{v})}\,\overline{S_{(v_1f_1+\cdots+v_kf_k)}(\boldsymbol{0})}\\&\quad+\overline{S_{(G)}(\boldsymbol{0})}\sum_{\boldsymbol{0}\neq\boldsymbol{v}=(v_1,\cdots,v_k)\in Z_m^k}S_{(G)}(\boldsymbol{v})S_{(v_1f_1+\cdots+v_kf_k)}(\boldsymbol{0})\\&\quad+\sum_{\boldsymbol{w}\in Z_m^n}\left[\left[\sum_{\boldsymbol{0}\neq\boldsymbol{v}=(v_1,\cdots,v_k)\in Z_m^k}S_{(G)}(\boldsymbol{v})S_{(v_1f_1+\cdots+v_kf_k)}(\boldsymbol{w})\right]\cdot\sum_{\boldsymbol{0}\neq\boldsymbol{v}=(v_1,\cdots,v_k)\in Z_m^k}\overline{S_{(G)}(\boldsymbol{v})}\,\overline{S_{(v_1f_1+\cdots+v_kf_k)}(\boldsymbol{w})}\right]u^{\boldsymbol{ws}}\right]\\&=\big|S_{(G)}(\boldsymbol{0})\big|^2+S_{(G)}(\boldsymbol{0})\sum_{\boldsymbol{0}\neq\boldsymbol{v}=(v_1,\cdots,v_k)\in Z_m^k}\overline{S_{(G)}(\boldsymbol{v})}\,\overline{S_{(v_1f_1+\cdots+v_kf_k)}(\boldsymbol{0})}+\\&\quad+\overline{S_{(G)}(\boldsymbol{0})}\sum_{\boldsymbol{0}\neq\boldsymbol{v}=(v_1,\cdots,v_k)\in Z_m^k}S_{(G)}(\boldsymbol{v})S_{(v_1f_1+\cdots+v_kf_k)}(\boldsymbol{0})\\&\quad+\sum_{\boldsymbol{0}\neq\boldsymbol{v}=(v_1,\cdots,v_k)\in Z_m^k}\big|S_{(G)}(\boldsymbol{v})\big|^2\left[\sum_{\boldsymbol{w}\in Z_m^n}\big|S_{(v_1f_1+\cdots+v_kf_k)}(\boldsymbol{w})\big|^2u^{\boldsymbol{ws}}\right]\\&\quad+\sum_{\substack{\boldsymbol{0}\neq\boldsymbol{v}=(v_1,\cdots,v_k)\in Z_m^k\\ \boldsymbol{v}\neq\boldsymbol{t}=(t_1,\cdots,t_k)\in Z_m^k\setminus\{\boldsymbol{0}\}}}S_{(G)}(\boldsymbol{v})\overline{S_{(G)}(\boldsymbol{t})}\left[\sum_{\boldsymbol{w}\in Z_m^n}S_{(v_1f_1+\cdots+v_kf_k)}(\boldsymbol{w})\overline{S_{(t_1f_1+\cdots+t_kf_k)}(\boldsymbol{w})}u^{\boldsymbol{ws}}\right]\\&=\big|S_{(G)}(\boldsymbol{0})\big|^2+S_{(G)}(\boldsymbol{0})\sum_{\boldsymbol{0}\neq\boldsymbol{v}=(v_1,\cdots,v_k)\in Z_m^k}\overline{S_{(G)}(\boldsymbol{v})}\,\overline{S_{(v_1f_1+\cdots+v_kf_k)}(\boldsymbol{0})}\\&\quad+\overline{S_{(G)}(\boldsymbol{0})}\sum_{\boldsymbol{0}\neq\boldsymbol{v}=(v_1,\cdots,v_k)\in Z_m^k}S_{(G)}(\boldsymbol{v})S_{(v_1f_1+\cdots+v_kf_k)}(\boldsymbol{0})\\&\quad+\sum_{\boldsymbol{0}\neq\boldsymbol{v}=(v_1,\cdots,v_k)\in Z_m^k}\big|S_{(G)}(\boldsymbol{v})\big|^2r_{\boldsymbol{v}f^{(k)}}(\boldsymbol{s})\\&\quad+\sum_{\substack{\boldsymbol{0}\neq\boldsymbol{v}=(v_1,\cdots,v_k)\in Z_m^k\\ \boldsymbol{v}\neq\boldsymbol{t}=(t_1,\cdots,t_k)\in Z_m^k\setminus\{\boldsymbol{0}\}}}S_{(G)}(\boldsymbol{v})\overline{S_{(G)}(\boldsymbol{t})}\,r_{\boldsymbol{v}f^{(k)},\boldsymbol{t}f^{(k)}}(\boldsymbol{s})\end{aligned}$$ 证毕

注 2 特别当 $m=2$ 时, 显然式(6)就是文献[3]中布尔“复合函数”的自相关函数计算公式, 易知 m 值“复合”逻辑函数的自相关函数计算公式与布尔“复合”函数的自相关函数计算公式在本质上是一致的。

定理 1，定理 2 得到的两个公式在 m 值“复合”逻辑函数的密码学性质研究中能够发挥重要的作用，下面我们先应用定理 1 的结论给出 m 值“复合”逻辑函数具备平衡性、相关免疫的条件。

定理 3　设 $G(\boldsymbol{z})$, $\boldsymbol{z}\in Z_m^k$ 是任一平衡的 k 元 m 值逻辑函数，若 k 维 m 值向量逻辑函数 $\boldsymbol{f}^{(k)}(\boldsymbol{x})=(f_1(\boldsymbol{x}),\cdots,f_k(\boldsymbol{x}))$, $\boldsymbol{x}\in Z_m^n$ 是平衡的，则“复合函数” $G(f_1(\boldsymbol{x}),\cdots,f_k(\boldsymbol{x}))$, $\boldsymbol{x}\in Z_m^n$ 是平衡的。

证明　由文献[4]可知，m 值逻辑函数 G 平衡，等价于对任意的 $\lambda\in Z_m\setminus\{0\}$，都有 $S_{(\lambda G)}(\boldsymbol{0})=0$，而 $\boldsymbol{f}^{(k)}(\boldsymbol{x})=(f_1(\boldsymbol{x}),\cdots,f_k(\boldsymbol{x}))$ 平衡，等价于对任意的 $\boldsymbol{0}\neq\boldsymbol{v}=(v_1,\cdots,v_k)\in Z_m^k$，有 $S_{(\boldsymbol{v}\boldsymbol{f}^{(k)})}(\boldsymbol{0})=0$，根据定理 1 中的式(2)就知，对 $\lambda\in Z_m\setminus\{0\}$，都有

$$S_{(\lambda G(f_1,\cdots,f_k))}(\boldsymbol{0})=S_{(\lambda G)}(\boldsymbol{0})+\sum_{\boldsymbol{v}=(v_1,\cdots,v_k)\in Z_m^k\setminus\{0\}}S_{(\lambda G)}(v)S_{(v_1f_1+\cdots+v_kf_k)}(\boldsymbol{0})=0$$

即“复合函数” $G(f_1(\boldsymbol{x}),\cdots,f_k(\boldsymbol{x}))$, $\boldsymbol{x}\in Z_m^n$ 是平衡的。证毕

定理 4　设 $G(\boldsymbol{z}),\boldsymbol{z}\in Z_m^n$ 为任一 k 元 m 值逻辑函数，若 k 维 m 值向量逻辑函数 $\boldsymbol{f}^{(k)}(\boldsymbol{x})=(f_1(\boldsymbol{x}),\cdots,f_k(\boldsymbol{x}))$, $\boldsymbol{x}\in Z_m^n$ 是 $t\left(1\le t\le n-1\text{为整数}\right)$ 阶相关免疫的，则“复合函数” $G(f_1(\boldsymbol{x}),\cdots,f_k(\boldsymbol{x})),\boldsymbol{x}\in Z_m^n$ 是 t 阶相关免疫的。

证明　若 k 维 m 值向量逻辑函数 $\boldsymbol{f}^{(k)}(\boldsymbol{x})=(f_1(\boldsymbol{x}),\cdots,f_k(\boldsymbol{x}))$ 是 t 阶相关免疫的，由引理 3，可知对任意的 $\boldsymbol{w}\in Z_m^n$，其汉明重量 $1\le W(\boldsymbol{w})\le t$，都有

$$S_{(v_1f_1+\cdots+v_kf_k)}(\boldsymbol{w})=0,\quad (v_1,\cdots,v_k)\in Z_m^k\setminus\{\boldsymbol{0}\}\tag{7}$$

那么对任意的 $\lambda\in Z_m\setminus\{0\}$ 及 $\boldsymbol{w}\in Z_m^n$，$1\le W(\boldsymbol{w})\le t$，利用式(7)和定理 1 中的式(3)，就有

$$S_{(\lambda G(f_1,\cdots,f_k))}(\boldsymbol{w})=\sum_{\boldsymbol{v}=(v_1,\cdots,v_k)\in Z_m^k\setminus\{\boldsymbol{0}\}}S_{(\lambda G)}(\boldsymbol{v})S_{(v_1f_1+\cdots+v_kf_k)}(\boldsymbol{w})=0$$

由引理 4 可知“复合函数” $G(f_1(\boldsymbol{x}),\cdots,f_k(\boldsymbol{x}))$ 是 t 阶相关免疫的。　　证毕

依据定理 2 的结论我们还可以对“复合函数”的自相关函数及其性质进行如下分析：

当 $G(z_1,\cdots,z_k)$ 自身平衡时，就有

$$r_{G(f_1,\cdots,f_k)}(\boldsymbol{s})=\sum_{\boldsymbol{0}\neq\boldsymbol{v}=(v_1,\cdots,v_k)\in Z_m^k}\left|S_{(G)}(\boldsymbol{v})\right|^2r_{\boldsymbol{v}\boldsymbol{f}^{(k)}}(\boldsymbol{s})+\sum_{\substack{\boldsymbol{0}\neq\boldsymbol{v}=(v_1,\cdots,v_k)\in Z_m^k\\ \boldsymbol{v}\neq\boldsymbol{t}=(t_1,\cdots,t_k)\in Z_m^k\setminus\{\boldsymbol{0}\}}}S_{(G)}(\boldsymbol{v})\overline{S_{(G)}(\boldsymbol{t})}r_{\boldsymbol{v}\boldsymbol{f}^{(k)},\boldsymbol{t}\boldsymbol{f}^{(k)}}(\boldsymbol{s}),\ \boldsymbol{s}\in Z_m^n$$

广义Bent函数具备很好的扩散特性，在密码设计中是非常有用处的一类逻辑函数，当 $G(z_1,\cdots,z_k)$ 自身平衡且对任意的 $\boldsymbol{0}\neq\boldsymbol{v}=(v_1,\cdots,v_k)\in Z_m^n$，$v_1f_1(x)+\cdots+v_kf_k(x)$，$\boldsymbol{x}\in Z_m^n$ 都是广义 Bent 函数时，就有

$$r_{G(f_1,\cdots,f_k)}(\boldsymbol{s})=\sum_{\substack{\boldsymbol{0}\neq\boldsymbol{v}=(v_1,\cdots,v_k)\in Z_m^k\\ \boldsymbol{v}\neq\boldsymbol{t}=(t_1,\cdots,t_k)\in Z_m^k\setminus\{\boldsymbol{0}\}}}S_{(G)}(\boldsymbol{v})\overline{S_{(G)}(\boldsymbol{t})}\cdot r_{\boldsymbol{v}\boldsymbol{f}^{(k)},\boldsymbol{t}\boldsymbol{f}^{(k)}}(\boldsymbol{s}),\ \boldsymbol{0}\neq\boldsymbol{s}\in Z_m^n$$

由定理 2 还可以知道：“复合”后所得函数的自相关性质不仅与 $f_1,\cdots,f_k$ 的非零线性组合的自相关函数的性质及其不同非零线性组合之间的互相关函数的性质有关，还与 G 和 $f_1,\cdots,f_k$ 的非零线性组合的谱性质有关。这就使得“复合”后所得函数的自相关性质变得较为复杂。事实上，即使 G 和 $f_1,\cdots,f_k$ 都取为自相关性质很好的广义 Bent 函数，也不能保证“复合”后的函数满足严格雪崩准则(见例 1)，选择何样的函数 G 和 $f_1,\cdots,f_k$ 能使“复合”后的函数具备较好的自相关性质还有待进一步研究。

例1　设 $m=3$，取二元广义 Bent 函数 $G(\boldsymbol{z})=z_1z_2$, $\boldsymbol{z}=(z_1,z_2)\in Z_3^2$，取 f_1,f_2 为两个广义 Bent 函数，其中 $f_1(\boldsymbol{x})=x_1x_2+x_3x_4$，$f_2(\boldsymbol{x})=x_1x_3+x_2x_4$，$\boldsymbol{x}=(x_1,x_2,x_3,x_4)\in Z_3^4$，由于“复合函数” $G(f_1(\boldsymbol{x}),f_2(\boldsymbol{x}))=(x_1x_2+x_3x_4)(x_1x_3+x_2x_4)$，$\boldsymbol{x}=(x_1,x_2,x_3,x_4)\in Z_3^4$ 在 $\boldsymbol{s}=(1,0,0,0)$ 处的差分函数有性质

$$P\{G(f^{(2)}(\boldsymbol{X}+\boldsymbol{s}))-G(f^{(2)}(\boldsymbol{X}))=0\}=11/27\neq1/3$$

其中 $\boldsymbol{X}=(X_1,X_2,X_3,X_4)$，$X_1,X_2,X_3,X_4$ 是相互独立且都具有“均匀分布”的 3 值随机变量. 而 m 是素数时，m 值逻辑函数 $f(\boldsymbol{x})$, $\boldsymbol{x}\in Z_m^n$ 满足严格雪崩准则等价于对任意的 $\boldsymbol{s}\in Z_m^n$, $W(\boldsymbol{s})=1$，差分函数 $f(\boldsymbol{x}+\boldsymbol{s})-f(\boldsymbol{x})$, $\boldsymbol{x}\in Z_m^n$ 都取值“均匀”[4]，故这里的“复合函数” $G(f_1,f_2)$ 不满足严格雪崩准则。

4　结束语

本文得到了 m 值“复合”逻辑函数的 Chrestenson 循环谱计算公式和自相关函数计算公式，以及有限个 m 值“复合”逻辑函数的非零线性和函数的 Chrestenson 循环谱计算公式，并对 m 值“复合”逻辑函数的有关密码学性质进行了分析。我们认为这些工作对于密码设计是很有意义的，使人们有可能更充分地利用多值“复合”逻辑函数的资源，根据实际需求选择具备一定性质的 G 和 $f_1,\cdots,f_k$ 来作“复合”，从而使相应的多层次非线性组合密钥流生成器具备要求的性能。对于选择何样的函数 G 和 $f_1,\cdots,f_k$ 能使“复合”后的函数具备较好的自相关性质还有待进一步研究。

参 考 文 献

[1] 冯登国. 频谱理论及其在密码学中的应用. 北京: 科学出版社, 2000，前言、第五章.

[2] Kishan Chand Gupta, Palash Sarkar. A General Correlation Theorem, in Cryptology ePrint Archive, report 2003/124, see http://ePrint.iacr.org/2003/124/ .

[3] 李迎东, 李世取. 布尔“复合函数”的 Walsh 循环谱和自相关函数. 应用数学, 2004, 17 (增): 22−28.

[4] 李世取, 曾本胜等. 密码学中的逻辑函数. 北京: 中软电子出版社, 2003，下篇第一章至第四章.

[5] 丁存生, 肖国镇. 流密码学及其应用. 北京: 国防工业出版社, 1994: 28−30.

李迎东：　女, 1973 年生，硕士生，研究方向为密码学.

李世取： 男, 1945 年生, 教授, 博士生导师, 研究方向为密码学.