学术论文

满足 k 阶严格雪崩准则的多值逻辑函数的谱特征

郭锦辉，李世取
（解放军信息工程学院信息研究系，郑州 450002）

[摘要] 给出了剩余类环 Z_m 上逻辑函数的 k 阶严格雪崩准则（SAC）的概念，用概率方法证明了 m 值逻辑函数满足高阶严格雪崩准则时一定满足低阶严格雪崩准则，并借助 Chrestenson 谱给出了 m 值逻辑函数满足 k 阶严格雪崩准则的一个充分必要条件。

[关键词] m 值逻辑函数；Chrestenson 谱；自相关函数；严格雪崩准则
[中图分类号] TN918.1 [文献标识码] A [文章编号] 1009－1742（2005）12－0045－04

在诸多密码攻击方法中有一种差分方法，是以输入的改变导致输出有相对较大改变为基础的一种攻击方法，针对此种攻击，Webster 和 Tavares 定义了布尔函数的严格雪崩准则（SAC）的概念：如果一个函数满足严格雪崩准则，那么当输入只有 1 b 改变时，输出改变的概率将是 1/2[1]，故以这样的布尔函数为非线性组合器产生的密钥流能够抗针对输入只改变 1 b 时的差分攻击。基于此，人们对满足严格雪崩准则的布尔函数的性质和构造等进行了一系列研究[2~5]，文献[2]得到了布尔函数满足严格雪崩准则的谱判别条件。

然而在选择性明文攻击中，密码破译者们又可以通过固定某些输入比特为常值后再作差分攻击，为此，Forré 对布尔函数的严格雪崩准则概念进行了拓展，给出了布尔函数满足 k 阶严格雪崩准则的定义，并得到了布尔函数满足 k 阶严格雪崩准则的谱判别条件[2]。以上工作对密码的设计者和分析者无疑都是有意义的。

依据实际应用的需要，近年来人们在密码学中对多值逻辑函数的有关性质和构造给予了更多的关注，将布尔函数的许多研究成果都拓广到了多值逻辑函数中，也特别给出了多值逻辑函数的严格雪崩准则的概念[6]，有不少成果问世（参见文献[6，7]）。但是，多值逻辑函数满足高阶严格雪崩准则的定义迄今尚未见到。笔者给出了剩余类环 Z_m 上逻辑函数满足 k 阶严格雪崩准则的定义，证明了 m 值逻辑函数满足高阶严格雪崩准则时一定满足低阶严格雪崩准则，考虑到谱在逻辑函数密码学性质研究中所发挥的作用，肖国镇、冯登国教授等在这方面做了很出色的工作[6]，笔者还利用反演公式得到了谱的一个分解公式，据此给出了 m 值逻辑函数满足 k 阶严格雪崩准则的一个谱判别条件，将文献[2]中的结果推广到了一般的 m 值逻辑函数。为记号简便，只就 $k=1$ 的情况给出 m 值逻辑函数满足 k 阶严格雪崩准则的主要结论的证明。

1 基本概念和预备知识

以下 $m \geqslant 2$ 是任一取定的正整数，且以 Z_m 记整数模 m 的剩余类环，又对任一取定的正整数 n，以 Z_m^n 表示 n 个 Z_m 的笛卡尔积。当 $\boldsymbol{w}=(w_1, w_2, \cdots, w_n) \in Z_m^n$ 时，称 $\boldsymbol{w}$ 的不为 0 元的分量个数为其汉明重量，且记为 $W(\boldsymbol{w})$。

定义 1[7] $Z_m^n \to Z_m$ 的任一映射 f 都为 Z_m^n 上的 n 个变元的 m 值逻辑函数，即若 $\boldsymbol{x}=(x_1, x_2, \cdots, x_n) \in Z_m^n$，则 $f(\boldsymbol{x})=f(x_1, x_2, \cdots, x_n) \in Z_m$。

[收稿日期] 2004－10－19；修回日期 2004－11－30
[作者简介] 郭锦辉（1979－），女，吉林长春市人，解放军信息工程大学信息工程学院硕士研究生

定义2[7] 设 $\boldsymbol{x}=(x_1, x_2, \cdots, x_n)\in Z_m^n$, $\boldsymbol{w}=(w_1, w_2, \cdots, w_n)\in Z_m^n$, 则 $\boldsymbol{x}$ 和 $\boldsymbol{w}$ 的点积定义为 $\boldsymbol{w}\cdot\boldsymbol{x}=w_1x_1+w_2x_2+\cdots+w_nx_n(\mathrm{mod}\ m)$, 则 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

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

称 $S_{(f)}(\boldsymbol{w})$, $\boldsymbol{w}\in Z_m^n$ 为 $f(\boldsymbol{x})$ 的 Chrestenson 循环谱。

定义3[6] 设 $f(\boldsymbol{x})$, $\boldsymbol{x}\in Z_m^n$ 是 m 值逻辑函数, 对 $\boldsymbol{x}=(x_1, x_2, \cdots, x_n)\in Z_m^n$, $\boldsymbol{s}=(s_1, s_2, \cdots, s_n)\in Z_m^n$ 记 $\boldsymbol{x}+\boldsymbol{s}=(x_1+s_1, x_2+s_2, \cdots, x_n+s_n)$, 称

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

为 $f(\boldsymbol{x})$ 的自相关函数。

定义4[7] 称 m 值逻辑函数 $f(\boldsymbol{x})$, $\boldsymbol{x}\in Z_m^n$ 是满足严格雪崩准则的, 若 $f(\boldsymbol{x})$ 的自相关函数 r_f 满足 $r_f(\boldsymbol{s})=0$, $\boldsymbol{s}\in Z_m^n$, $W(\boldsymbol{s})=1$。

定义5 设 $n\geqslant 2$, $1\leqslant k<n$, 称 n 元 m 值逻辑函数 $f(x_1, x_2, \cdots, x_n)$ 是满足 k 阶严格雪崩准则的, 如果取定 $f(x_1, x_2, \cdots, x_n)$ 的 n 个变元 x_1, x_2, $\cdots$, x_n 中的任意 k 个后, 所得 $n-k$ 元的 m 值逻辑函数都是满足严格雪崩准则的。

下设 $\boldsymbol{X}=(X_1, X_2, \cdots, X_n)$ 中的 X_1, X_2, $\cdots$, X_n 是定义在同一概率空间 (Ω, F, P) 上相互独立且都具有均匀分布的 m 值随机变量, 即对任意的 $(a_1, a_2, \cdots, a_n)\in Z_m^n$, 都有

$$P\{X_1=a_1, X_2=a_2, \cdots, X_n=a_n\}=$$
$$P\{X_1=a_1\}\cdot P\{X_2=a_2\}\cdot\cdots\cdot P\{X_n=a_n\},$$

和 $P\{X_i=a\}=1/m$, $a\in Z_m$, $1\leqslant i\leqslant n$, 则易知对任一 m 值逻辑函数 $f(x_1, \cdots, x_n)$, $f(X_1, \cdots, X_n)$ 也为 (Ω, F, P) 上的 m 值随机变量。

在上述记号的意义下, 关于 m 值逻辑函数的自相关函数的概率表示式已有下面的结果:

定理1[7] 对任一 m 值逻辑函数 $f(\boldsymbol{x})$, $\boldsymbol{x}\in Z_m^n$, 都有

$$r_f(\boldsymbol{s})=\sum_{r\in Z_m}u^rP\{f(\boldsymbol{X}+\boldsymbol{s})-f(\boldsymbol{X})=r\},$$
$$\boldsymbol{s}\in Z_m^n。$$

定理2[8] (反演公式) 对任一 m 值逻辑函数 $f(\boldsymbol{x})$ 与其 Chrestenson 循环谱的关系为

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

关于 m 值逻辑函数满足严格雪崩准则的 Chrestenson 谱判别条件, 又已有下面的结果:

定理3[7] m 值逻辑函数 $f(\boldsymbol{x})$, $\boldsymbol{x}\in Z_m^n$ 满足严格雪崩准则的充分必要条件是对所有的 $1\leqslant j\leqslant n$, 只要 $s_j\in Z_m\setminus\{0\}$, 就都成立

$$\sum_{w\in Z_m^n}|S_{(f)}(w)|^2\cdot u^{w_j\cdot s_j}=0。$$

2 主要结果

定理4 如果 m 值逻辑函数 $f(\boldsymbol{x})$, $\boldsymbol{x}\in Z_m^n$ 满足 k 阶严格雪崩准则, 那么 $f(\boldsymbol{x})$ 必定满足 $k-1$ 阶严格雪崩准则 (0阶严格雪崩准则即原来意义下的严格雪崩准则)。

证明 为记号简单, 只给出满足1阶严格雪崩准则必定满足严格雪崩准则的证明。

设 m 值逻辑函数 $f(x_1, x_2, \cdots, x_n)$ 满足1阶严格雪崩准则, 根据定义知, 此时对任意的 $1\leqslant i\leqslant n$ 和 $a\in Z_m$, $n-1$ 元 m 值逻辑函数

$$f_{i:a}(\boldsymbol{x}(i))=f(x_1, \cdots, x_{i-1}, a, x_{i+1}, \cdots, x_n)$$

都要满足严格雪崩准则, 再根据定理1, 即知对任意的 $a\in Z_m$ 和

$$\boldsymbol{s}^*=(s_1, \cdots, s_{i-1}, s_{i+1}, \cdots, s_n)\in Z_m^{n-1}$$
且 $W(\boldsymbol{s}^*)=1$,
$$r_{fi:a}(s_1, \cdots, s_{i-1}, s_{i+1}, \cdots, s_n)=$$
$$\sum_{r\in Z_m}u^rP\{f(X_1+s_1, \cdots, X_{i-1}+s_{i-1},$$
$$a, X_{i+1}+s_{i+1}, \cdots, X_n+s_n)-f(X_1, \cdots,$$
$$X_{i-1}, a, X_{i+1}, \cdots, X_n+s_n)=r\}=0$$

都成立。

今设 $\boldsymbol{s}=(s_1, \cdots, s_n)\in Z_m^n$ 且 $W(\boldsymbol{s})=1$, 即 $\boldsymbol{s}$ 中仅有一个分量不为0, 不妨设

$$s_1\neq 0, 即\ \boldsymbol{s}=(s_1, 0, \cdots, 0),$$

于是有

$$r_f(s_1, 0, \cdots, 0)=$$
$$\sum_{r\in Z_m}u^rP\{f(X_1+s_1, X_2, X_3, \cdots, X_n)-$$
$$f(X_1, X_2, X_3, \cdots, X_n)=r\}=$$
$$\sum_{r\in Z_m}\sum_{a\in Z_m}u^rP\{f(X_1+s_1, a, X_3, \cdots, X_n)-$$
$$f(X_1, a, X_3, \cdots, X_n)=r, X_2=a\}=0$$
$$\sum_{r\in Z_m}\sum_{a\in Z_m}u^rP\{f(X_1+s_1, a, X_3, \cdots, X_n)-$$

$$f(X_1, a, X_3, \cdots, X_n) = r\}P\{X_2 = a\} = \frac{1}{m}\sum_{r\in Z_m}\Big[\sum_{a\in Z_m}u^rP\{f(X_1 + s_1, a, X_3, \cdots, X_n) - f(X_1, a, X_3, \cdots, X_n) = r\}\Big] = 0,$$

由此即易知 $f(\boldsymbol{x})$ 满足严格雪崩准则。

定理 4 告知，m 值逻辑函数满足 $k(\geqslant 1)$ 阶严格雪崩准则的一个必要条件是它必须满足通常意义下的严格雪崩准则。

根据 m 值逻辑函数满足 $k(\geqslant 1)$ 阶严格雪崩准则的定义不难得到如下引理：

引理 1　m 值逻辑函数 $f(\boldsymbol{x})$，$\boldsymbol{x} \in Z_m^n$ 满足 k 阶严格雪崩准则的充分必要条件是对所有的正整数 $1 \leqslant i \leqslant n$ 和 $a \in Z_m$，取定 $x_i = a$ 后所得 $n-1$ 元函数 $f(x_1, \cdots, x_{i-1}, a, x_{i+1}, \cdots, x_n)$ 满足 $k-1$ 阶严格雪崩准则。

注意：对任意的 $1 \leqslant i \leqslant n$，$n$ 元 m 值逻辑函数 $f(\boldsymbol{x})$，$\boldsymbol{x} \in Z_m^n$ 都可表示为

$$f(x_1, \cdots, x_{i-1}, x_i, x_{i+1}, \cdots, x_n) = \sum_{r\in Z_m} I_{\{a\}}(x_i) f_{i;a}(\boldsymbol{x}(i)), (x_1, x_2, \cdots, x_n) \in Z_m^n,$$

其中

$$f_{i;a}(\boldsymbol{x}(i)) = f(x_1, \cdots, x_{i-1}, a, x_{i+1}, \cdots, x_n),$$

$$I_{\{a\}}(x_i) = \begin{cases} 1, & x_i = a, \\ 0, & x_i \neq a, \end{cases} \quad x_i \in Z_m, a \in Z_m。$$

又记

$$\boldsymbol{w} = (w_1, \cdots, w_{i-1}, k, w_{i+1}, \cdots, w_n) \in Z_m^n$$

为 $(k, \boldsymbol{w}(i))$，而记

$$\boldsymbol{w}(i) = (w_1, \cdots, w_{i-1}, w_{i+1}, \cdots, w_n),$$

$$\boldsymbol{X}(i) = (X_1, \cdots, X_{i-1}, X_{i+1}, \cdots, X_n)。$$

定理 5　设 $f(x_1, \cdots, x_n)$ 是任一 m 值逻辑函数，则对任意的 $1 \leqslant i \leqslant n$，当 f 表示为

$$f(x_1, \cdots, x_{i-1}, a, x_{i+1}, \cdots, x_n) = \sum_{r\in Z_m} I_{\{a\}}(x_i) f_{i;a}(x(i))$$

时，就有

$$S_{(f_{i;a})}(\boldsymbol{w}(i)) = \sum_{k\in Z_m} u^{ak} S_{(f)}(k, \boldsymbol{w}(i)),\ a \in Z_m \tag{1}$$

证明　根据 m 值逻辑函数 Chrestenson 谱定义式和反演公式可知，对任意取定的 $a \in Z_m$ 和 $(k, \boldsymbol{w}(i)) \in Z_m^n$ 都有

$$S_{(f_{i;a})}(\boldsymbol{w}(i)) = \frac{1}{m^{n-1}}\sum_{x^r\in Z_m^{n-1}} u^{f_{i;a}(\boldsymbol{x}(i))} u^{-\boldsymbol{w}(i)\cdot x^r} = \frac{1}{m^{n-1}}\sum_{x^r\in Z_m^{n-1}}\sum_{k\in z_m, v(i)\in Z_m^{n-1}} S_{(f)}(k, \boldsymbol{v}(i)) u^{ka + v(i)\cdot x^r} \cdot u^{-w(i)\cdot x^r} = \frac{1}{m^{n-1}}\sum_{k\in z_m, v(i)\in Z_m^{n-1}} u^{ka} S_{(f)}(k, \boldsymbol{v}(i)) \cdot \sum_{x^r\in Z_m^{n-1}} u^{[v(i)-w(i)]x^r} = \sum_{k\in Z_m} u^{ka} S_{(f)}(k, \boldsymbol{w}(i))。$$

特别在 $m = 2$，$i = n$ 时，注意到 $u = -1$，定理 5 中的式 (1) 即是布尔函数性质研究中发挥了重要作用的那个著名公式

$$S_{f_{i;1}}(\boldsymbol{w}(n)) = S_{(f)}(0, \boldsymbol{w}(n)) - S_{(f)}(1, \boldsymbol{w}(n)),$$

$$S_{f_{i;0}}(\boldsymbol{w}(n)) = S_{(f)}(0, \boldsymbol{w}(n)) + S_{(f)}(1, \boldsymbol{w}(n))。$$

对任一 $\boldsymbol{w} = (w_1, \cdots, w_{i-1}, w_i, w_{i+1}, \cdots, w_n) \in Z_m^n$ 再记

$$w_{i_1, a_1, \cdots, i_k, a_k} = (w_1, \cdots, w_{i_1-1}, w_{i_1} + a_1, w_{i_1+1}, \cdots, w_{i_k-1}, w_{i_k} + a_k, w_{i_k+1}, \cdots, w_n) \in Z_m^n。$$

根据定理 5 和引理 1，可以得到 m 值逻辑函数满足 k 阶严格雪崩准则的如下谱判别条件：

定理 6　m 值逻辑函数 $f(\boldsymbol{x})$，$\boldsymbol{x} \in Z_m^n$ 满足 k 阶严格雪崩准则的充分必要条件是对所有的 $1 \leqslant i_1 < \cdots < i_k \leqslant n$，$1 \leqslant j \leqslant n$ 且 $\{j\} \subset \{1, 2, \cdots, n\} \setminus \{i_1, \cdots, i_k\}$，$s_j \in Z_m \setminus \{0\}$ 和对任意的 $(a_1, \cdots, a_k) \in Z_m^k$，

$$\sum_{w\in Z_m^n} [S_{(f)}(\boldsymbol{w}) \bar{S}_{(f)}(w_{i_1, a_1, \cdots, i_k, a_k})] u^{w_{j^s j}} = 0$$

都成立。

特别当 $k = 1$ 时，m 值逻辑函数 $f(\boldsymbol{x})$，$\boldsymbol{x} \in Z_m^n$ 满足 1 阶严格雪崩准则的充分必要条件是对所有的 $i, j \in \{1, 2, \cdots, n\}$ 且 $i \neq j$，$s_j \in Z_m \setminus \{0\}$ 和对任意的 $a \in Z_m$，

$$\sum_{w\in Z_m^n} S_{(f)}(\boldsymbol{w}) \bar{S}_{(f)}(w_{i,a}) u^{w_{j^s j}} = 0$$

都同时成立。

证明　为记号简单，只就 $k = 1$ 的情况给出 m 值逻辑函数满足 k 阶严格雪崩准则的主要证明，一般结论可再根据引理 1 由数学归纳法得到。

由定义 5 和定理 3 可知，$f(\boldsymbol{x})$ 满足 1 阶严格雪崩准则的充分必要条件，是对所有的 $i, j \in \{1, 2, \cdots, n\}$ 且 $i \neq j$，$s_j \in Z_m \setminus \{0\}$ 和对任意的 $a \in Z_m$，都有

$$\sum_{w(i)\in Z_m^{n-1}} |S_{(f_i;a)}(\boldsymbol{w}(i))|^2 u^{w_{j^s j}} = 0。$$

而根据定理 5，在上述记号的意义下，对所有 的 a

$\in Z_m$，就有

$$\sum_{w(i)\in Z_m^{n-1}} |S_{(f_i:a)}(w(i))|^2 u^{w_j s_j} = \sum_{w(i)\in Z_m^{n-1}} \Big[\sum_{r\in Z_m} u^{ar} S_{(f)}(k, w(i))\Big] \cdot \Big[\sum_{r\in Z_m} u^{-ar} \bar{S}_{(f)}(r, w(i))\Big] u^{w_j s_j} = \sum_{w(i)\in Z_m^{n-1}} \Big[\sum_{k\in Z_m} |S_{(f)},(k, w(i))|^2 u^{w_j s_j} + \sum_{w(i)\in Z_m^{n-1}} \Big[\sum_{\substack{k,r\in Z_m \\ k\neq r}} u^{a(k-r)} S_{(f)},(k, w(i)) \cdot \bar{S}_{(f)}(r, w(i))\Big] u^{w_j s_j} = \sum_{w\in Z_m^n} |S_{(f)}(w)|^2 u^{w_j s_j} + \sum_{w(i)\in Z_m^{n-1}} \Big[\sum_{\substack{k,r\in Z_m \\ k\neq r}} u^{a(k-r)} S_{(f)},(k, w(i)) \cdot \bar{S}_{(f)}(r, w(i))\Big] u^{w_j s_j} \quad (2)$$

记

$$S_0 = \sum_{w\in Z_m^n} |S_{(f)}(w)|^2 u^{w_j s_j} = \sum_{w\in Z_m^n} S_{(f)}(w)) \bar{S}_{(f)}(w_{i,0}) u^{w_j s_j},$$

$$S_1 = \sum_{w(i)\in Z_m^{n-1}} \sum_{\substack{k\in Z_m \\ k-r=1}} S_{(f)}(k, w(i)) \cdot \bar{S}_{(f)}(r, w(i))] u^{w_j s_j} = \sum_{w\in Z_m^n} S_{(f)}(w) \bar{S}_{(f)}(w_{i,m-1}) u^{w_j s_j},$$

$$\vdots$$

$$S_{m-1} = \sum_{w(i)\in Z_m^{n-1}} \sum_{\substack{k\in Z_m \\ k-r=m-1}} S_{(f)}(k, w(i)) \cdot \bar{S}_{(f)}(r, w(i))] u^{w_j s_j} = \sum_{w\in Z_m^n} S_{(f)}(w) \bar{S}_{(f)}(w_{i,1}) u^{w_j s_j},$$

则对所有的 $a \in Z_m$，式 (2) 就是

$$\sum_{w(i)\in Z_m^{n-1}} |S_{(f_{i:a})}(w(i))|^2 u^{w_j s_j} = S_0 + u^a S_1 + \cdots + u^{a(m-1)} S_{m-1} \quad (3)$$

因而，若 $S_0 = S_1 = \cdots = S_{m-1} = 0$，则由式 (3) 即知对所有的 $a \in Z_m$，都有

$$\sum_{w(i)\in Z_m^{n-1}} |S_{(f_{i:a})}(w(i))|^2 \cdot u^{w_j s_j} = 0。$$

反之，若对所有的 $a \in Z_m$，式(3) 都成立，则在式(3) 中取遍 $a \in Z_m$，就得到关于 S_0，S_1，…，S_{m-1} 的方程组

$$\begin{cases} S_0 + S_1 + \cdots + S_{m-1} = 0, \\ S_0 + uS_1 + \cdots u^{m-1} S_{m-1} = 0, \\ \vdots \\ S_0 + u^{m-1} S_1 + \cdots + u^{(m-1)(m-1)} S_{m-1} = 0, \end{cases}$$

解之即得

$$S_0 = S_1 = \cdots = S_{m-1} = 0。$$

特别在 $m = 2$ 时，注意到 $u = 1$ 及对任意的 $w \in Z_2^n$，$S_{(f)}(w)$ 都为实数，定理 6 中结论为：布尔函数 $f(x)$，$x \in Z_2^n$ 满足 k 阶严格雪崩准则的充分必要条件，是对所有的 $1 \leqslant i_1 < \cdots < i_k \leqslant n$，$1 \leqslant j \leqslant n$ 且 $\{j\} \subset \{1, 2, \cdots, n\} \setminus \{i_1, \cdots, i_k\}$，$s_j \in Z_2 \setminus \{0\}$ 和对任意的 $(a_1, \cdots, a_k) \in Z_2^k$，$\sum_{w\in Z_2^n} [S_{(f)}(w) S_{(f)}(w_{i_1,a_1,\cdots,i_k,a_k})] \cdot (-1)^{w_j} = 0$ 都成立。这是文献[2]中的主要结果。

3 结语

在剩余类环 Z_m 上给出了 m 值逻辑函数的 k 阶严格雪崩准则 (SAC) 的概念，并借助 Chrestenson 谱给出了 m 值逻辑函数满足 k 阶严格雪崩准则的一个充分必要条件，此外，依据定理 6 的结论，还可以给出满足 k 阶严格雪崩准则的 m 值逻辑函数的更多的递归构造方法，用变元个数少的逻辑函数构造变元个数多且满足 k 阶严格雪崩准则的逻辑函数，更好地在密码设计中使用逻辑函数的资源，因而是有实际意义的。

参考文献

[1] Webster A F, Tavares S E. On the design of S-boxes [A]. Advances in Cryptology, Crypto'85 [C]. Springer-Verlag, 1986. 523～534

[2] Forre R. The strict avalanche criterion: properties of Boolean functions and extended definition [A]. Advances in Crytology-Crypt '88 [C]. Springer-Verlag, 1990. 450～468

[3] Cusick W. Boolean functions satisfying a higher order strict avalanche criterion [A]. Advances in Crytology-Eurocrypt '93 [C]. Springer-Verlag, 1994. 86～95

[4] Youssef A M, Cusick T W, Stanica P, Tavares S E. New bounds on the number of functions satisfying the strict avalanche criterion [A]. In Third Annual Workshop on Selected Areas in Cryptography [C]. 1996

[5] 冯登国，肖国镇. 满足 k 次扩散准则的布尔函数的谱特征 [J]. 电子科学学刊，1996，(4)：385～390

(下转第 102 页)

（上接第48页）

[6] 冯登国. 频谱理论及其在密码学中的应用 [M]. 北京：科学出版社，2000

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

[8] 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

The Strict Avalanche Criterion of Order k Spectral Properties of m-Valued Logical Functions

Guo Jinhui, Li Shiqu

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

[**Abstract**] Many cryptographic properties of m-valued logical functions are often described by their Chrestenson cyclic spectrums and auto-correlation functions, so Chrestenson cyclic spectrums and auto-correlation functions play important roles in properties and constructions for m-valued logical functions. In this paper, in residue class ring Z_m, the concept of the strict avalanche criterion of order k of m-valued logical functions is presented. Then, by applying probabilistic thought and methods, the rule that a m-valued logical function fulfills the SAC of lower order if it fulfills the SAC of higher order is proved. Finally, by Chrestenson cyclic spectrums, a necessary and sufficient condition on a m-valued logical function is given, which fulfills the strict avalanche criterion of order k.

[**Key words**] m-valued logical function; Chrestenson cyclic spectrum; auto-correlation function; the strict avalanche criterion