第15卷 第6期
1993年11月

电子科学学刊
JOURNAL OF ELECTRONICS

Vol. 15, No. 6
Nov., 1993

严格择多逻辑函数的密码学特征

冯登国　　肖国镇
(西安电子科技大学信息保密研究所，西安 710071)

摘要　本文主要讨论了当 $n=2^m+1(m>1)$ 时，n 阶严格择多逻辑函数的代数正规形式中，所有的阶为 $k((n+1)/2\leqslant k\leqslant n-1)$ 的非线性项都出现，从而从密码学角度来说，这种函数有好的密码学特征.

关键词　密码学;严格择多逻辑函数;谱

1. 引言

在密码学中，为了提高密钥流序列的线性复杂度，人们将好的序列进行非线性组合或滤波。组合或波函数的选择是非常重要的，它直接影响着密钥流序列的性能。文献[1]中指出为了克服“相关攻击”，组合或滤波函数应选取相关免疫阶较高的函数。但一个函数的相关免疫阶和非线性阶之间存在着一种制约关系，所以在选取组合或滤波函数时应对这两方面进行折衷。文献[2]中指出为了克服“BAA 攻击”，组合或滤波函数应选取较稳定的函数，即函数的谱较均匀的函数。文献[3]中指出 n 元布尔函数 $f(x_1,x_2,\cdots,x_n)$ 是 m 阶相关免疫的，当且仅当 $S_f(\omega)=0$，对任意 ω，$1\leqslant W_H(\omega)\leqslant m$，$W_H(\omega)$ 表示 ω 的汉明重量。由第一种谱 $S_f(\omega)$ 和第二种谱 $S_{(f)}(\omega)$ 之间的关系易知，n 元布尔函数 $f(x_1,x_2,\cdots,x_n)$ 是 m 阶相关免疫的，当且仅当 $S_{(f)}(\omega)=0$，对任意 ω，$1\leqslant W_H(\omega)\leqslant m$. 在这里我们把条件 $S_{(f)}(\omega)=0$ 减弱到 $|S_{(f)}(\omega)|\leqslant\varepsilon$，$\varepsilon$ 是足够小的正数。满足这种条件的函数就避免了相关免疫阶与非线性阶之间的折衷，但它可以经受“相关攻击”。对足够小的正数 ε，当 n 充分大时，n 阶弯曲函数便满足这个条件，遗憾的是 n 阶弯曲函数的非线性阶不超过 $n/2$。本文将指出严格择多逻辑 (SML) 函数作为组合或滤波函数具有好的密码学特征，特别地，当 $n=2^m+1$，$(m>1)$ 时，SML 函数更是理想的组合或滤波函数.

2. 严格择多逻辑函数的谱特征

定义 1　设 n 是正奇数，n 元布尔函数

$$g(x)=g(x_1,x_2,\cdots,x_n)=\begin{cases}1, & 若\ W_H(x)>n/2\\0, & 若\ W_H(x)<n/2\end{cases}$$

1992.07.23 收到，1992.12.10 定稿.

冯登国　男，1966年生，硕士生，现从事密码研究.

肖国镇　男，1945 年生，教授，博士生导师，现从事密码学、编码学、信息论、应用数学等方面的教学和研究.

称为 SML 函数。

定义 2 设 $f(x)$ 是 n 元布尔函数，称

$$S_{(f)}(\omega)=2^{-n}\sum_{x\in GF^{n}(2)}(-1)^{\omega\cdot x+f(x)}$$

为 $f(x)$ 的第二种谱变换。$\omega\cdot x$ 表示 ω 与 x 的内积。

引理 1 设 n 是正奇数，$g(x)$ 是 SML 函数，则

$$S_{(g)}(\omega)=\begin{cases}0, & \text{若 } W_H(\omega) \text{ 为偶数}\\ (-1)^{\frac{l-1}{2}}\dfrac{(n-l)!(l-1)!}{\left(\frac{n-1}{2}\right)!\left(\frac{n-l}{2}\right)!\left(\frac{l-1}{2}\right)!2^{n-1}}, & \text{若 } W_H(\omega)=l<n/2,\ l \text{ 为奇数}\\ (-1)^{n-\frac{l+1}{2}}\dfrac{(l-1)!(n-l)!}{\left(\frac{n-1}{2}\right)!\left(\frac{l-1}{2}\right)!\left(\frac{n-l}{2}\right)!2^{n-1}}, & \text{若 } W_H(\omega)=l>n/2,\ l \text{ 为奇数}\end{cases}$$

引理 2 设 n 是正奇数，$g(x)$ 是 SML 函数，则

$$\max_{\omega\in GF^{n}(2)}|S_{(g)}(\omega)|=\binom{n-1}{\frac{n-1}{2}}\Big/2^{n-1}$$

其中 $\binom{n}{k}\triangleq n!/(k!(n-k)!)$。

由高等数学易知

$$\lim_{n\to\infty}\binom{n-1}{\frac{n-1}{2}}\Big/2^{n-1}=0$$

对足够小的正数 ε，当 n 充分大时，

$$\max_{\omega\in GF^{n}(2)}|S_{(g)}(\omega)|\leqslant\varepsilon$$

说明当 n 充分大时，n 阶 SML 函数是较稳定的。这种函数选作为组合或滤波函数是比较理想的。它不仅可以经受“BAA 攻击”，而且可以经受“相关攻击”。再者，适当变换 SML 函数的谱的次序可得到更合适的组合或滤波函数。

3. 严格择多逻辑函数的非线性阶

引理 3 设 n 为正奇数，$g(x)$ 是 SML 函数，则在 $g(x)$ 的代数正规形式中阶小于、等于 $(n-1)/2$ 的项不出现。

引理 4 设 n 为正奇数，$g(x)$ 是 SML 函数，则在 $g(x)$ 的代数正规形式中所有的阶为 k 的非线性项出现，当且仅当 $\varepsilon_k=\sum_{i=0}^{k-\frac{n+1}{2}}\binom{k}{i}$ 是奇数，$(n+1)/2\leqslant k\leqslant n-1$。

由引理 4 易知，在 $g(x)$ 的代数正规形式中所有的阶为 $(n+1)/2$ 的非线性项都出现。

引理 5　设 n 为正奇数，$g(x)$ 是 SML 函数，则 $\deg(g) \leqslant n-1$，$\deg(g)$ 表示 $g(x)$ 的次数。

定理 1　设 n 为正奇数，$g(x)$ 是 SML 函数，则在 $g(x)$ 的代数正规形式中所有的阶为 k 的非线性项都出现，当且仅当 $\begin{pmatrix} k-1 \\ \frac{n-1}{2} \end{pmatrix}$ 是奇数，$(n+1)/2 \leqslant k \leqslant n-1$

证明　由引理 5 知，只须证明对 k，$(n+1)/2 \leqslant k \leqslant n-1$，$\varepsilon_k = \sum_{i=0}^{k-\frac{n+1}{2}} \binom{k}{i}$ 为奇数，当且仅当 $\begin{pmatrix} k-1 \\ \frac{n-1}{2} \end{pmatrix}$ 为奇数。

由于

$$
\begin{aligned}
\varepsilon_k &= \sum_{i=0}^{k-\frac{n+1}{2}} \binom{k}{i} = 1 + \sum_{i=1}^{k-\frac{n+1}{2}} \binom{k}{i} \\
&= 1 + \sum_{i=1}^{k-\frac{n+1}{2}} \left[\binom{k-1}{i} + \binom{k-1}{i-1}\right] \\
&= 1 + \sum_{i=1}^{k-\frac{n+1}{2}} \binom{k-1}{i} + \sum_{i=1}^{k-\frac{n+1}{2}} \binom{k-1}{i-1} \\
&= 2\varepsilon_{k-1} + \begin{pmatrix} k-1 \\ k-\frac{n+1}{2} \end{pmatrix} = 2\varepsilon_{k-1} + \begin{pmatrix} k-1 \\ \frac{n-1}{2} \end{pmatrix}
\end{aligned}
$$

注意在上述证明过程中用了如下两个组合数公式：

$$
\binom{n-1}{i-1} + \binom{n-1}{i} = \binom{n}{i}, \quad \binom{n}{i} = \binom{n}{n-i}
$$

所以 ε_k 为奇数，当且仅当 $\begin{pmatrix} k-1 \\ \frac{n-1}{2} \end{pmatrix}$ 为奇数，利用引理 5 即得此定理。

引理 6　设 $n = 2^m + 1$，$(m > 1)$，对任意的 k，$2^{m-1} + 1 \leqslant k \leqslant 2^m$，$\binom{k-1}{2^{m-1}}$ 为奇数。

证明　对 k 用归纳法证明之。当 $k = 2^m + 1$ 时，$\binom{k-1}{2^{m-1}} = \binom{2^{m-1}}{2^{m-1}} = 1$ 为奇数。

假设对 k 有 $\binom{k-1}{2^{m-1}}$ 为奇数，则对 $k+1 \leqslant 2^m$ 有 $\binom{k}{2^{m-1}} = \frac{k}{k-2^{m-1}}\binom{k-1}{2^{m-1}}$，

因 $k \leqslant 2^m - 1$，所以 $k = 2^t p$，其中 $t \leqslant m-1$，p 为奇数，从而 $k/(k - 2^{m-1}) = p/(p - 2^{m-1-t})$，故由假设知，$\binom{k}{2^{m-1}}$ 为奇数．由归纳法知，引理 6 为真．

定理 2 设 $n = 2^m + 1$，$m > 1$，$g(x)$ 是 n 阶 SML 函数，则 $g(x_1, x_2, \cdots, x_n) = \sum_{i=\frac{n+1}{2}}^{n-1} f_i^n(x_1, x_2, \cdots, x_n)$．其中 $f_k^n(x_1, x_2, \cdots, x_n) = \sum_{1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant n} x_{i_1} x_{i_2} \cdots x_{i_k}$ 称为基本对称布尔函数．

证明 由定理条件和引理 6，定理 1 易证此定理成立．

由定理 2 知，当 $n = 2^m + 1$，$(m > 1)$ 时，n 阶 SML 函数的代数正规形式中，所有的 $k((n+1)/2 \leqslant k \leqslant n-1)$ 阶非线性项都出现，把这种函数选作组合或滤波函数时，能保证密钥流序列有较大的线性复杂度．从而，从非线性阶来看，这种函数亦是理想的组合或滤波函数．

4. 结束语

从前面的讨论知，SML 函数无论从它的谱值还是从它的非线性阶来看都是比较理想的．将 SML 函数的谱分布适当调序便可得出更理想的函数来．特别地，当 $n = 2^m + 1$ 时，这种阶数的 SML 函数作为组合或滤波函数是更合适的函数，能保证密钥流序列有好的性能．

参考文献

[1] T. Siegenthaler, *IEEE Trans, on IT*, **IT-30**(1984)5, 776—780.
[2] C. Ding, D. Xiao, W. Shan, The Stability Theory of Stream Ciphers, Springer-Verlag Press, (1991), Germany, pp. 61—80.
[3] Xiao Guo-Zhen, James. L. Massey, *IEEE Trans. on IT*, **IT-34**(1988)34. 431—433.
[4] R. C. Titsworth, Optimal Ranging Codes, IEEE Trans. on Space Electronics and Telemetry, March 1964, 19—30.

CRYPTOLOGICAL CHARACTERIZATION OF THE STRICT MAJORITY LOGIC FUNCTIONS

Feng Dengguo Xiao Guozhen

(Xidian University Xi'an 710071)

Abstract It is proved that in the algebraic normal form of the strict majority logic function with order $n = 2^m + 1 (m > 1)$, all the nonlinear terms of k-th order, $(n+1)/2 \leqslant k \leqslant n-1$, must appear. Threrfore, from the view of cryptology, such strict majority logic function has good characteristics.

Key words Cryptology; Strict majority; Logic function; Spectrum