一类平衡前馈序列的构造与性质 [1]

金君娥 * 李 超 * ** 吴 翊 *

*(国防科技大学数学与系统科学系 长沙 410073)
**(东南大学移动通信国家重点实验室 南京 210018)

摘 要: 该文采用 m 序列选控传统前馈密码系统的方法，在继承了 Bent 函数谱值均匀优点的同时，使得产生的序列具有理想的平衡性、大的周期和高的线性复杂度，且能抵抗现有的线性逼近攻击和相关攻击.

关键词: 前馈流密码， Walsh 谱，平衡，周期，线性复杂度
中图分类号: TN918 **文献标识码**: A **文章编号**: 1009-5896(2004)09-1395-06

Construction and Properties of Balance Feedforword Sequences

Jin Jun-e* Li Chao* ** Wu Yi*

*(*Dept of Math. and Sys. Sci., NUDT, Changsha* 410073, *China*)

**(*State Key Lab of Mobile Communication, Southeast Univ., Nanjing* 210018, *China*)

Abstract By using an m-sequence controlling a traditional feedforward stream cipher, this paper constructs a new feedforward network whose sequences have ideal balance, large period and linear complexity, it can also resist on linear approaching attack and correlation attack, at the same time it inherits the virtues of Bent functions's even Walsh spectra.

Key words Feedforward stream cipher, Walsh spectra, Balance, Period, Linear complexity

1 引言

前馈网络密码系统是一种重要的非线性流密码体制，其基本模型是用一个 m 序列作为驱动序列，通过适当抽头进入非线性前馈函数，函数的输出序列即为前馈序列。它的目的是希望在保持 m 序列优良的伪随机特性的同时，提高序列的线性复杂度以抵抗 Berlekamp-Massey(B-M) 算法等的攻击 [1,2] 。同时为了抵抗基于 Walsh 谱的相关攻击，又要求前馈函数有很均匀的谱值分布，于是 Bent 函数在前馈网络中有了广泛的应用 [3,4] 。但是 Bent 函数也有它的弱点，除了其代数次数受限 (不超过变元数的一半) 外，它产生的序列是不平衡的。而平衡是一条密钥流序列的基本要求 [5] ，本文正是从保证平衡性这一点出发，构造了一类新型的前馈密码系统. 分析表明，新的系统不但确保了平衡，且克服了一般前馈密码系统周期和线性复杂度等难分析的困难，即满足了密钥序列的 3 个基本条件：周期大；平衡性好；线性复杂度高。并且输出序列对输入序列的信息泄漏是可控的，也就是说它的安全性可根据需要自由掌握。

2 概念和模型

定义 1 $\forall \omega \in F_2^n$ ，函数 $f(x): F_2^n \to F_2$ 的 Walsh 谱 $S_{(f)}(\omega) = 2^{-n} \sum_{x \in F_2^n} (-1)^{f(x)+\omega \cdot x}$.

Walsh 谱 $S_{(f)}(\omega)$ 揭示了 $f(x)$ 和 $\omega \cdot x$ 的相关度，即有 $P(f(x) = \omega \cdot x) = 1/2 + S_{(f)}(\omega)/2$ ，它是密码分析的有力工具，其大小和分布直接影响密码系统的安全性。 Walsh 谱的另一个重要

[1] 2003-04-24 收到， 2003-11-10 改回
东南大学移动通信国家重点实验室开放基金 (A0307) 和国防科技大学基础研究基金 (JC 02-02-007) 资助项目

性质是能量守恒，即 $\sum_{\omega\in F_2^n} S_{(f)}^2(\omega)=1$.

定义 2 称 n 元布尔函数 $f(x):F_2^n\to F_2$ 是 Bent 函数，如果其谱值是绝对均匀的，即 $\forall\omega\in F_2^n, |S_{(f)}(\omega)|=2^{-n/2}$.

对一个 n 元 Bent 函数 $f(x)$ 而言， $P(f(x)=0)=1/2+S_{(f)}(0)/2=1/2\pm 2^{-1-n/2}$ ，所以是不平衡的。Bent 函数有许多特殊的性质，如变元个数为偶数，代数次数不超过变元数一半等。

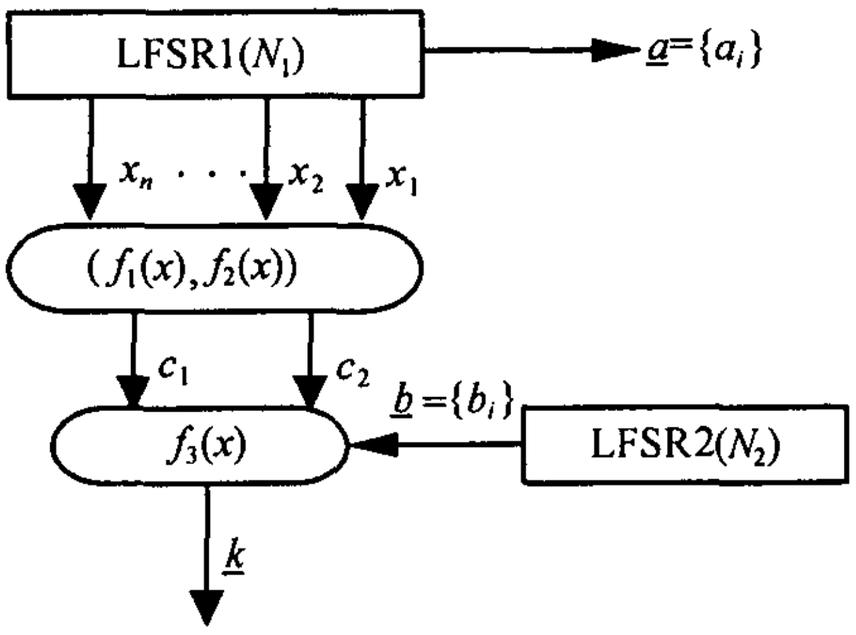

图 1 新前馈系统的模型

模型如图 1 所示， LFSR1 和 LFSR2 分别是级数为 N_1 和 N_2 的线性反馈移位寄存器，其反馈多项式是本原多项式 $g_1(x)$, $g_2(x)$ ，输出序列是 m 序列 $\underline{a}=\{a_i\}$ 和 $\underline{b}=\{b_i\}$ 。 $x_1,x_2,\cdots,x_n$ 是 n 个抽头且跨距 $0=t_1<t_2<\cdots<t_n<N_1$ ，前馈函数 $f_1(x)$ 和 $f_2(x)$ 是 n 元 Bent 函数，各自的输出序列是 $\underline{c}_1=\{c_{1,i}\}$ 和 $\underline{c}_2=\{c_{2,i}\}$ ，一般的前馈系统直接将序列 $\underline{c}_1$ 和 $\underline{c}_2$ 用作密钥流。而本文的模型继续利用 $\underline{b}$ 对 $\underline{c}_1$ 和 $\underline{c}_2$ 选择，具体就是如果 $b_i=0$ ，则 $k_i=c_{1,i}$ ，如果 $b_i=1$ ，则 $k_i=c_{2,i}+l$ ，其中 l 由 $f_1(x)$ 和 $f_2(x)$ 唯一确定：如果 $\mathrm{sgn}[S_{(f_1)}(0)S_{(f_2)}(0)]=1$, $l=1$ ，否则 $l=0$ 。可以写成公式 $k_i=(1+b_i)c_{1,i}+b_i(l+c_{2,i})$ ，其中 $l=\frac{1+\mathrm{sgn}(S_{(f_1)}(0)\cdot S_{(f_2)}(0))}{2}$ 。

我们约定函数 $f_1(x)$ 和 $f_2(x)$ 是独立的，且与 LFSR2 也独立。这样选控函数 f_3 可表为 $f_3(x_1,\cdots,x_n,y)=(1+y)f_1(x_1,\cdots,x_n)+y(l+f_2(x_1,\cdots,x_n))$, y 即是 LFSR2 的输出。

3 性质

定理 1 在上述模型中，输出序列 $\underline{k}$ 是平衡的，即 $P(f_3=1)=P(f_3=0)=1/2$.

证明 将 $l+f_2(x_1,\cdots,x_n)$ 重新记成 $f_2(x_1,\cdots,x_n)$ ，则 $S_{(f_1)}(0)=-S_{(f_2)}(0)$ 。将 $f_3(x_1,\cdots,x_n,y)$ 简记为 $f_3=(1+y)f_1+y\cdot f_2$ ，记 $S_{(f_1)}(0)=S$ ，由 Walsh 谱的性质，我们有 $P(f_1=0)=1/2+S/2$, $P(f_1=1)=1/2-S/2$ ，而 $P(f_2=0)=1/2-S/2$, $P(f_2=1)=1/2+S/2$ ，而由 m 序列的性质我们可以认为 $P(y=1)=P(y=0)=1/2$ 。于是

$$\begin{aligned}P(f_3=1)&=P(f_1=1)P(1+y+y\cdot f_2=1|f_1=1)+P(f_1=0)P(y\cdot f_2=1|f_1=0)\\&=P(f_1=1)P(1+y+y\cdot f_2=1)+P(f_1=0)P(y\cdot f_2=1)\\&\qquad\text{(这里利用了 } f_1 \text{ 和 } f_2 \text{ 及 } y \text{ 的独立性)}\\&=P(f_1=1)P(y(1+f_2)=0)+P(f_1=0)P(y=1)P(f_2=1)\\&=P(f_1=1)[1-P(y=1)P(f_2=0)]+P(f_1=0)P(y=1)P(f_2=1)\\&=(1/2-S/2)-(1/2-S/2)\cdot 1/2\cdot(1/2-S/2)+(1/2+S/2)\cdot 1/2\cdot(1/2+S/2)\\&=1/2-S/2-1/2\cdot[(1/2-S/2)^2-(1/2+S/2)^2]=1/2-S/2+S/2=1/2\end{aligned}$$

于是 $P(f_3=0)=1-1/2=1/2$. 证毕

不难从直观上理解，我们引入参数 l 的目的就是要得到两个有正好相反的 0,1 优势的序列，经过 0,1 均衡近乎随机的 m 序列的选择而达到平衡。与平衡问题平行的一个问题是关于游程分

布的问题，本文没有从理论上进行研究，但试验表明新序列的游程分布呈现理想的 1/2 递减趋势，几乎符合随机序列的游程分布特点 [6]，比传统的前馈序列要好得多。关于周期，有

定理 2　分别记序列 $\underline{c}_1, \underline{c}_2, \underline{b}$ 的周期为 P_1, P_2, P_3，则序列 $\underline{k}$ 的最小周期 $P = [P_1, P_2, P_3]$ 是 P_1, P_2, P_3 的最小公倍数。

证明　令 $T = [P_1, P_2, P_3]$，即 T 是能同时被 P_1, P_2, P_3 整除的最小正整数。显然，T 是 $\underline{k}$ 的一个周期。如果有 $P < T$ 也是 $\underline{k}$ 的周期，即 $\forall i, k_{i+P} = k_i$。记 $P = P_1 q_1 + r_1$, $P = P_2 q_2 + r_2$, $P = P_3 q_3 + r_3$，其中 $q_i \in Z, 0 \le r_i < P_i$。于是

$$\begin{aligned} k_{i+P} &= (1 + b_{i+P})c_{1,i+P} + b_{i+P}(l + c_{2,i+P}) \\ &= (1 + b_{i+P_3 q_3 + r_3})c_{1,i+P_1 q_1 + r_1} + b_{i+P_3 q_3 + r_3}(l + c_{2,i+P_2 q_3 + r_2}) \\ &= (1 + b_{i+r_3})c_{1,i+r_1} + b_{i+r_3}(l + c_{2,i+r_2}) \\ &= k_i = (1 + b_i)c_{1,i} + b_i(l + c_{2,i}) \end{aligned}$$

得 $(1 + b_{i+r_3})c_{1,i+r_1} + b_{i+r_3}(l + c_{2,i+r_2}) = (1 + b_i)c_{1,i} + b_i(l + c_{2,i})$。注意到我们的讨论都是在二元域上的，等式可变形为 $(c_{1,i+r_1} + l + c_{2,i+r_2})b_{i+r_3} + (c_{1,i} + l + c_{2,i})b_i + (c_{1,i+r_1} + c_{1,i}) = 0$ 对任何 i 都成立。如果不是 $r_1 = r_2 = r_3 = 0$，这个式子就表明序列 $\underline{b}, \underline{c}_1, \underline{c}_2$ 有这样一种潜在的非常严格的制约关系：$(L^{r_1}\underline{c}_1 + l \cdot 1 + L^{r_2}\underline{c}_2)L^{r_3}\underline{b} + (\underline{c}_1 + l \cdot 1 + \underline{c}_2)\underline{b} + L^{r_1}\underline{c}_1 + \underline{c}_1 = 0, l \cdot 1$ 表示全 1 列和 l 的积序列。而实际情况是这 3 条序列相互独立，等式左边的组合序列不可能出现严格全零，所以有 $r_1 = r_2 = r_3 = 0$。也就是说 $P_i | P, i = 1, 2, 3$，于是 $T = [P_1, P_2, P_3]$ 是序列 $\underline{k}$ 的最小周期。　　证毕

众所周知，讨论一般前馈序列的密码性质是困难的，如知道它的周期是输入 m 序列周期 $P_a = 2^{N_1} - 1$ 的因子，但具体的大小和前馈函数有密切关系，下限难界定。也就是说上文中的 P_1, P_2 可能不好确定，但是 P_3 是 m 序列 $\underline{b}$ 的周期，很显然，$P_3 = 2^{N_2} - 1$。这样，新序列的周期 $P \ge P_3$，当然 $P | P_3 \cdot P_a$。于是我们就可以用 LFSR2 的级数来保证序列 $\underline{k}$ 的周期，这是新序列较之于传统序列的又一优点。同样要计算一般前馈序列 $\underline{c}_1$ 和 $\underline{c}_2$ 的线性复杂度或估计出好的线性复杂度下界是困难的，本文也不打算分析序列 $\underline{c}_1$ 或 $\underline{c}_2$ 等传统前馈序列的线性复杂度，而是考虑新序列 $\underline{k}$ 的线性复杂度与传统前馈序列 $\underline{c}_1$ 和 $\underline{c}_2$ 的线性复杂度之间的关系。考虑到组合函数 $f_3 = (1 + y)f_1 + y \cdot (f_2 + l)$ 正是一种常用的提高非线性度的构造方法，从直观上看，新序列 $\underline{k}$ 的线性复杂度应该比直接由 f_1 和 f_2 产生的传统前馈序列 $\underline{c}_i$ 的要高，我们的几个试验也确实表明了这一点。理论上有下列结果：

引理 1[2]　基于 F_2 上 n 级 m 序列 $\{a_i\}$ 的前馈序列 $\{b_i\}$ 的线性复杂度 $L(\{b_i\})$ 满足 $L(\{b_i\}) \le \sum_{j=1}^{k} \binom{n}{j}$，其中 k 为非线性前馈布尔函数 $f(x_0, x_1, \cdots, x_{n-1})$ 的次数。

定理 3　设模型中序列 $\underline{c}_1 = \{c_{1,i}\}$ 和 $\underline{c}_1 + \underline{c}_2 = \{c_{1,i} + c_{2,i}\}$ 的线性复杂度分别为 L_1 和 L_2，则当 $(N_1, N_2) = 1$ 时，序列 $\underline{k}$ 的线性复杂度达到上界 $L_1 + l \cdot N_2 + N_2 \cdot L_2$。

证明　因为 $k_i = (1 + b_i)c_{1,i} + b_i(l + c_{2,i}) = c_{1,i} + l \cdot b_i + b_i(c_{1,i} + c_{2,i})$，即序列 $\underline{k}$ 是由 3 条序列 $\underline{c}_1, l \cdot \underline{b}$ 和 $\underline{b} \wedge (\underline{c}_1 + \underline{c}_2)$ 相加而成，符号 $\wedge$ 表示两个序列的哈达玛乘积，所以

$$L(\underline{k}) \le L(\underline{c}_1) + L(l \cdot \underline{b}) + L(\underline{b} \wedge (\underline{c}_1 + \underline{c}_2)) \le L(\underline{c}_1) + l \cdot L(\underline{b}) + L(\underline{b}) \cdot L(\underline{c}_1 + \underline{c}_2) = L_1 + l \cdot N_2 + N_2 \cdot L_2$$

下面证明当 $(N_1, N_2) = 1$ 时，$L(\underline{k})$ 达到极大。需要证两个方面：(1) 设序列 $\underline{b}$ 和 $(\underline{c}_1 + \underline{c}_2)$ 的极小多项式是 $m_1(x)$ 和 $m_2(x)$，为保证 $L(b \wedge (\underline{c}_1 + \underline{c}_2)) = L(\underline{b}) \cdot L(\underline{c}_1 + \underline{c}_2)$，需 $m_1(x)$ 和 $m_2(x)$ 二者之中至少有一个仅有单根，且所有的根乘积 $z(m_1) \cdot z(m_2)$ 互不相同；(2) 设序列 $\underline{c}_1$,

$l\cdot\underline{b}$ 和 $b\wedge(\underline{c}_1+\underline{c}_2)$ 的极小多项式分别为 $h_1(x),h_2(x),h_3(x)$，为保证 3 条序列和的线性复杂度等于序列复杂度之和，需证明这 3 个极小多项式两两互素。

先证第一点。不妨设 α 是 N_1 级本原多项式 $g_1(x)$ 的一个本原根，$\alpha^{2^{N_1}-1}=1$，则 $\alpha,\alpha^2,\alpha^{2^2},\cdots,\alpha^{2^{N_1-1}}$ 是 $g_1(x)$ 的 N_1 个不同的根，域 $F_{2^{N_1}}=\{0,1,\alpha,\alpha^2,\alpha^3,\cdots,\alpha^{2^{N_1}-2}\}$；同样设 β 是 $g_2(x)$ 的一个本原根，$\beta^{2^{N_2}-1}=1$，则 $\beta,\beta^2,\beta^{2^2},\cdots,\beta^{2^{N_2-1}}$ 是 $g_2(x)$ 的 N_2 个不同的根，域 $F_{2^{N_2}}=\{0,1,\beta,\beta^2,\beta^3,\cdots,\beta^{2^{N_2}-2}\}$，由于 $(N_1,N_2)=1$，所以 $F_2^{N_1}$ 和 $F_2^{N_2}$ 的公共子域是 F_2。显然 $m_1(x)=g_2(x)=\prod_{i=0}^{N_2-1}(x-\beta^{2^i})$ 只有单根。而序列 $(\underline{c}_1+\underline{c}_2)$ 是函数为 $f(x)=f_1(x)+f_2(x)=\sum_{i=1}^{n}c_ix_i+\sum_{i\neq j}c_{i,j}x_ix_j+\cdots+\sum_{i_1\neq i_2\neq\cdots\neq i_r}c_{i_1,i_2,\cdots,i_r}x_{i_1}x_{i_2}\cdots x_{i_r}$ 的前馈序列，其中 $r=\deg(f_1+f_2)\le n/2$，记函数 $x_{i_1}x_{i_2}\cdots x_{i_J}$ $(J\le r)$ 产生的序列为 $\underline{u}=\{u_i\}=\left\{\prod_{j=1}^{J}Tr_{r_1}^{N_1}(r_j\alpha^i)\right\}$，其中 $r_1,r_2,\cdots,r_J$ 由各抽头决定，则

$$u_i=\prod_{j=1}^{J}\sum_{l=0}^{N_1-1}(r_j\alpha^i)^{2^i}=\sum_{k_1=0}^{N_1-1}\sum_{k_2=0}^{N_1-1}\cdots\sum_{k_J=0}^{N_1-1}(k_1,k_2,\cdots,k_J)\alpha^{c(k)i}$$

其中 $r(k_1,k_2,\cdots,k_J)=\prod_{j=1}^{J}r_j^{2^{kj}}$，$c(k)=\sum_{j=1}^{J}2^{kj}\bmod(2^{N_1}-1)$，由于 $c(k)$ 的二进制表示中至多 $J(\le r)$ 位取值为 1，于是由序列的根表示定理，令 $F_r(x)=\prod_{W(i)\le r,i\in F_2^{N_1}}(x-\alpha^i)$ $(W(i)$ 表示 i 的汉明重量)，显然它仅有单根，是序列 $\underline{u}$ 的一个生成多项式，从而也是多条不同 $\underline{u}$ 叠加序列 $(\underline{c}_1+\underline{c}_2)$ 的一个生成多项式。现在我们说明：(1) $\beta^{2^i}\cdot\alpha^j\neq\beta^{2^i}\cdot\alpha^k,\ j\neq k$；(2) $\beta^{2^i}\cdot\alpha^k\neq\beta^{2^j}\cdot\alpha^k,\ i\neq j$；(3) $\beta^{2^i}\cdot\alpha^j\neq\beta^{2^k}\cdot\alpha^l,\ i\neq k,j\neq l$。(1) 和 (2) 成立是由于 $F_r(x)$ 和 $m_1(x)$ 仅有单根；若存在 $i\neq k,j\neq l$，使得 $\beta^{2^i}\cdot\alpha^j=\beta^{2^k}\cdot\alpha^l$ 成立，则变形为 $\beta^{2^i-2^k}=\alpha^{l-j}$，由前面讨论知 $F_2^{N_1}$ 和 $F_2^{N_2}$ 的公共子域是 $F_2=\{0,1\}$，则 $\beta^{2^i-2^k}=0$ 或 1，而对于 $0\le i,k<N_2,i\neq k$ 来说这是不成立的，所以 (3) 也成立。于是根乘积 $z(m_1)\cdot z(F_r)$ 互不相同，而 $m_2(x)|F_r(x)$，所以乘积 $z(m_1)\cdot z(m_2)$ 也互不相同。

第二点的证明同样利用函数的根，不妨设 $l=1$，此时 $h_2(x)=g_2(x)$，(当 $l=0$ 时 $h_2(x)=1$ 自然与 $h_1(x),h_3(x)$ 互素)，由上面证明中的结果有 $h_1(x),h_2(x)$ 和 $h_3(x)$ 都只有单根，不妨设 $h_1(x)$ 的根集合为 $S_1=\{\alpha^{i_1},\cdots,\alpha^{i_{L_1}}\}$，其中 i_j 满足 $0<W(i_j)\le\deg(f_1)$，$j=1,2,\cdots,L_1$，$h_2(x)$ 的根集合为 $S_2=\{\beta,\beta^2,\beta^{2^2},\cdots,\beta^{2^{N_2-1}}\}$，序列 $(\underline{c}_1+\underline{c}_2)$ 的极小多项式的根集合为 $S=\{\alpha^{j_1},\cdots,\alpha^{j_{L_2}}\}$，同样 i_j 满足 $0<W(i_j)\le\deg(f_1+f_2),j=1,2,\cdots,L_2$，则 $h_3(x)$ 的根集合是 $S_3=\{x\cdot y|x\in S_2,y\in S\}$。要证 $h_1(x),h_2(x)$ 与 $h_3(x)$ 互素，只需证 $S_i\cap S_j=\phi,i\neq j,i,j=1,2,3$，证明过程完全同上面根乘积互不相同的证明，略。

定理 3 说明当选取适当的 Bent 型前馈函数 $f_1(x),f_2(x)$，使得 $\deg f_1(x)=\deg(f_1(x)+f_2(x))\ge\deg f_2(x)$，且序列 $\underline{c}_1$ 和 $(\underline{c}_1+\underline{c}_2)$ 的线性复杂度达到最大值 $L=\sum_{j=1}^{r}\binom{N_1}{j},(r=\deg f_1(x))$，则只要 $(N_1,N_2)=1$，序列 $\underline{k}$ 的线性复杂度就达到最大值 $L(N_2+1)+lN_2$，可以看出 l 的取值对最大值影响不大。试验表明这样的 $f_1(x),f_2(x)$ 是容易选取的。

最后说明新序列的安全性是完全可控的。

定理 4 $\forall\omega\in F_2^{n+1}$，模型中的选控函数 $f_3(x_1,x_2,\cdots,x_n,y)$ 的 Walsh 谱值 $S_{(f_3)}(\omega)$ 为 0，或者为 $\pm2^{-n/2}$，其中 n 是前馈系统的抽头数。

证明　$f_3(x_1,x_2,\cdots,x_n,y)=(1+y)f_1(x_1,x_2,\cdots,x_n)+y(l+f_2(x_1,x_2,\cdots,x_n)$, $\forall\omega\in F_2^{n+1}$，记 $\omega=(\omega_1,\omega_2)$, $\omega_1\in F_2^n$, $\omega_2\in F_2$,

$$
\begin{aligned}
S_{(f_3)}(\omega)&=2^{-(n+1)}\sum_{x\in F_2^{n+1}}(-1)^{f_3(x)+\omega\cdot x}\\
&=2^{-(n+1)}\sum_{x\in F_2^n,y\in F_2}(-1)^{(1+y)f_1(x)+y(l+f_2(x))+\omega_1\cdot x+\omega_2\cdot y}\\
&=2^{-(n+1)}\sum_{x\in F_2^n,y\in F_2}(-1)^{f_1(x)+\omega_1\cdot x+y(f_1(x)+l+f_2(x)+\omega_2)}\\
&=2^{-(n+1)}\left(\sum_{x\in F_2^n,y=0}(-1)^{f_1(x)+\omega_1\cdot x}+\sum_{x\in F_2^n,y=1}(-1)^{f_2(x)+l+\omega_1\cdot x+\omega_2}\right)\\
&=2^{-(n+1)}[2^nS_{(f_1)}(\omega_1)+(-1)^{\omega_2}\cdot 2^nS_{(l+f_2)}(\omega_1)]\\
&=(1/2)\cdot[S_{(f_1)}(\omega_1)+(-1)^{\omega_2}\cdot S_{(l+f_2)}(\omega_1)]
\end{aligned}
$$

注意到 $f_2(x)+l$ 还是 n 元 Bent 函数，有 $|S_{(f_1)}(\omega_1)|=|S_{(l+f_2)}(\omega_1)|=2^{-n/2}$．于是，当 $S_{(f_1)}(\omega_1)$ 和 $(-1)^{\omega_2}\cdot S_{(l+f_2)}(\omega_1)$ 的符号相异时，$S_{(f_3)}(\omega)=0$；两者符号相同时，$S_{(f_3)}(\omega)=S_{(f_1)}(\omega_1)=\pm 2^{-n/2}$．　证毕

由定理 4 和 Walsh 谱的能量守恒性质就可得出如下结果：

推论　$\#\{S_{(f_3)}(\omega)=0|\omega\in F_2^{n+1}\}=\#\{S_{(f_3)}(\omega)=\pm 2^{-n/2}|\omega\in F_2^{n+1}\}=2^n$．

定理 4 和推论表明，与一般前馈系统相比，增加 m 序列的选控后，虽然谱点数增加了一倍，但谱值非零点的数目不增加，也不会有某个点的谱值增大。而一般的多输出前馈网络，就可能出现几个 Bent 型前馈函数的线性组合是非 Bent 函数，导致组合函数的最大谱值增加，降低了系统的安全性 [7−9]．相比之下，我们就可以控制抽头数来严格控制相关性，从而控制各个端口的泄漏信息，来抵抗现有的基于谱值的线性逼近攻击和相关攻击。

4 例子

设 LFSR1 和 LFSR2 的反馈多项式分别是本原多项式 $g_1(x)=x^{17}+x^3+1$ 和 $g_2(x)=x^{11}+x^2+1$，前馈函数 $f_1(x)=x_1x_6+x_2x_4+x_3x_5+x_1x_2$, $f_2(x)=x_1x_5+x_2x_6+x_3x_4+x_2x_3$ 是 Bent 函数，$x_1,\cdots,x_6$ 分别抽自移存器的第 1, 2, 4, 7, 11, 16 级，即抽头跨距分别为 $t_1=0, t_2=1, t_3=3, t_4=6, t_5=10, t_6=15$，则用 B-M 算法可求得 $L(\underline{c}_1)=L(\underline{c}_2)=153$ (等于上界 153)，等价的抽头数是 48，$L(\underline{k})=1847$ (等于上界 $153+11+11\times 153$)，等价的抽头数是 880。

在下面的讨论中，序列 $\underline{c}_1$ 和 $\underline{c}_2$ 在的长度为 $(2^{17}-1)$，$\underline{k}$ 的长度为 $(2^{17}-1)(2^{11}-1)$，都是其周期的整数倍。序列 0, 1 百分比：$\underline{c}_1(\underline{c}_2$ 同)：56.25%~43.75%; 而 $\underline{k}$：50.0031%~49.9969%。游程分布如表 1 所示。

表 1 序列 $\underline{c}_1, \underline{c}_2$ 和 $\underline{k}$ 的游程分布

序列 $\underline{c}_1$ 的 0,1 游程分布			序列 $\underline{c}_2$ 的 0,1 游程分布			序列 $\underline{k}$ 的 0,1 游程分布		
序列号	0 游程	1 游程	序列号	0 游程	1 游程	序列号	0 游程	1 游程
1	14592	18176	1	14081	17664	1	33539584	33536001
2	7616	7362	2	7360	7616	2	16474560	16540351
3	3936	3231	3	4704	3616	3	8671328	8639264
4	2264	1528	4	2184	1608	4	4240136	4255208
5	1240	720	5	1336	712	5	2143832	2063328
6	952	352	6	880	296	6	1038912	1021912
7	330	232	7	466	124	7	485538	515284
8	179	62	8	373	51	8	245957	250030
9	175	47	9	120	30	9	119189	127787
10	137	16	10	93	16	10	61329	63373
11	117	12	11	57	7	11	27696	33322
12	42	1	12	34	3	12	14489	15429
13	72	3	13	26	1	13	7525	7991
14	17	3	14	10	0	14	3254	3836
15	11	0	15	8	0	15	1541	1842
16	34	0	16	3	0	16	835	822
18	2	0	17	4	0	17	458	432
19	8	0	18	4	0	18	196	214
20	1	0	21	2	0	19	127	102
21	3	0				20	54	37
22	4	0				21	32	20
23	1	0				22	19	13
24	2	0				23	6	5
25	1	0				24	2	2
27	1	0				25	5	1
30	3	0				26	2	2
33	2	0				30	2	0
47	1	0						
81	1	0						

参 考 文 献

[1] Rueppel R A. Analysis and Design of Stream Ciphers. Berlin: Springer-Verlag, 1986: 54–141.

[2] 丁存生，肖国镇. 流密码学及其应用. 北京：国防工业出版社， 1994: 130–160.

[3] Siegenthaler T. Correlation-immunity of nonlinear combining functions for cryptographic applications. *IEEE Trans. on Info. Theory.*, 1984, IT-30(5): 776–780.

[4] 李世鹏，朱近康. 一类新的性能优越的伪随机序列. 电子学报， 1993, 21(1): 41–51.

[5] 杨义先，林须端. 编码密码学. 北京：人民邮电出版社， 1992: 531–538.

[6] 张申如，梅文华，王庭昌等. 非周期 q 元均匀随机序列的游程特性. 通信学报， 2000, 21(1): 45–48.

[7] 胡一平，冯登国. 多输出前馈函数的一种相关分析方法. 电子科学学刊， 1998, 20(6): 787–793.

[8] 孙林红，叶顶峰，吕述望. 前馈网络的信息泄漏. 通信学报， 2002, 23(8): 19–23.

[9] 金君娥，李超，吴翊. 前馈网络的信息泄漏与收集. 通信学报， 2004, 25(3): 1–7.

金君娥： 女， 1977 年生，硕士生，主要研究方向是密码学和信息安全.

李 超： 男， 1966 年生，教授，博士生导师，主要研究方向是密码学和信息安全.

吴 翊： 男， 1948 年生，教授，博士生导师，主要研究方向是动态系统分析与数据处理.