多输出前馈函数的一种相关分析方法 [1]

胡一平 冯登国 *

(中国科技大学研究生院 信息安全国家重点实验室 北京 100039)
*(中国科学院软件所 信息安全工程研究中心 北京 100080)

摘 要 本文提出了分析多输出前馈网络的一种方法，该方法的基本思想是收集输入信息在多个输出端上的信息泄漏，从而达到更充分地利用所有泄漏的信息的目的．作为应用，利用文中给出的方法分析了一类重要的多输出前馈网络——多输出 Bent 函数，并用一个具体实例说明了这种方法的全过程．

关键词 多输出变换，择多原理，Bent 函数，谱，相关分析
中图号 TN918

1 引 言

前馈网络系统是一种重要的流密码生成器，因此，人们已对一些特殊的前馈模型特别是单输出情形下的前馈网络模型进行了大量研究 [1-3]，得出了一系列重要的结果．然而，对于一般的多输出前馈网络系统而言，目前比较深入的研究结果尚不多见．由于多输出前馈网络各个输出分量之间存在着一定的制约关系，就使得该系统本身存在着不同于单输出前馈网络的一些特点，尤其是在多输出前馈网络中，同一输入信息往往会在多个输出端上均有所泄漏．这时，如何收集这些泄漏的信息，并使得其在密码分析中得以应用，是一个非常值得考虑的问题．

本文针对图 1 所示的模型讨论了上述问题，给出了解决这个问题的一种方法．作为应用，利用文中给出的方法分析了一类重要的多输出前馈网络——多输出 Bent 函数，并用一个具体实例说明了这种方法的全过程．

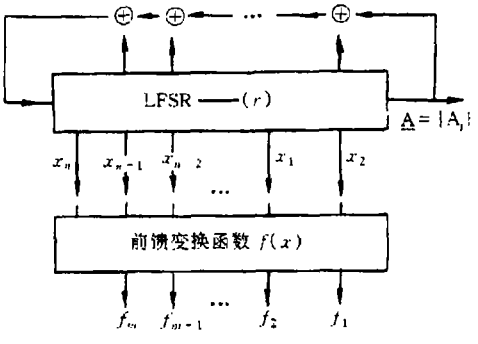

图 1 多输出前馈网络系统

文中我们均限制在二元域 F_2 上讨论，前馈函数 $f(x) = (f_1(x), f_2(x), \cdots, f_m(x))$ 是从 $GF(2)^n$ 到 $GF(2)^m$ 的函数；LFSR-(r) 表示 GF(2) 上级数为 $r \geq n$ 的线性反馈移位寄存器，

[1] 1997-04-07 收到，1998-01-20 定稿
国家自然科学基金资助项目 (项目编号：69703012)

输出序列为 $\underline{a}=\{a_j: a_j\in F_2\}$. 假定 x_i 和 x_1 之间的抽头跨距分别为 $t_i(i=2,3,\cdots,n)$, $t_i<r$, 并且如果 $i>j$, 则有 $t_i>t_j$. 约定 $t_1=0$, 不失一般性, 可假定 x_1 抽自移位寄存器的第一级.

2 多输出前馈网络的信息泄漏问题和特点

造成多输出前馈网络信息泄漏的主要原因仍然是输出与输入之间有一定的相关性, 因而在研究多输出前馈网络的信息泄漏时, 必须从相关性开始. 本文拟采用频谱技术来研究多输出前馈网络的相关特性.

对于任意的 $\mu\in F_2^m$, 令 $\mu*f(x)=\mu_1f_1\oplus\mu_2f_2\oplus\cdots\oplus\mu_mf_m$, 则它也是 n 个变元的布尔函数. $\mu*f(x)$ 在点 $v\in F_2^n$ 处的 Walsh 谱定义为

$$S(\mu*f)(v)=2^{-n}\sum_{x\in F_2^n}(-1)^{\mu*f(x)\oplus v\cdot x}$$

我们把 $S(\mu*f)(v)$ 记为 $S_{(f)}(\mu,v)$, 即 $S_{(f)}(\mu,v)=S_{(\mu*f)}(v)$, 则容易得到 $P_{(\mu*f=v\cdot x)}=1/2+S_{(f)}(\mu,v)/2$. 由此可见 $S_{(f)}(\mu,v)$ 刻划了 $\mu*f$ 与 $v*x$ 之间的相关程度. 于是称 $S_{(f)}(\mu,v)$ 为 $\mu*f$ 与 $v*x$ 之间的相关系数. 令 $c=\max\{|S_{(f)}(\mu,v)|:\mu\in F_2^m\backslash\{O\},v\in F_2^n\}$; $U=\{\mu\in F_2^m\backslash\{0\}:$ 存在$v\in F_2^n$,使得$|S_{(f)}(\mu,v)|=c\}$; $V=\{v\in F_2^n:$ 存在$\mu\in F_2^m\backslash\{0\}$,使得$|S_{(f)}(\mu,v)|=c\}$. 从 U 中选取一个极大线性无关组扩充为 F_2^n 的一组基, 不妨设为 $\mu_1,\mu_2,\cdots,\mu_m$. 设 $C(v)=\prod_{i=1}^m(1/2+|S_{(f)}(\mu_i,v)|/2)$, 找出使得 $C(v_0)=\max_{v\in V}C(v)$ 的 $v_0\in V$. 一般地讲, 这个 v_0 不仅使得集合 $\{|S_{(f)}(\mu_i,v_0)|\}_{1\le i\le m}$ 中至少有一个达到最大值 c, 而且这些值中还会有多个是大于 0 的值. 这说明 μ_i*f $(1\le i\le m)$ 中同时会有多个表达式均与输入的线性组合 $v_0\cdot x$ 有一定的相关性. 而 m 个关系式 $\mu_i*f(x)=v_0\cdot x(1\le i\le m)$ 在通常情况下是相互独立的, 所以, 从信息论的角度出发, $v_0\cdot x$ 在多个输出端上的信息泄漏将比任何一个输出端上的信息泄漏要大. 这正是按上述方法选择 v_0 的理由, 它也是多输出前馈网络信息泄漏的一个特点. 对于上述求出的 v_0 , 不妨设 $\{\mu_i*f\}_{(1\le i\le m)}$ 中的 k 个函数 $\mu_1*f,\mu_2*f,\cdots,\mu_k*f$ $(k\le m)$ 所产生的序列 $z_i=(z_{ij})$ $(1\le i\le k)$ 与 $v_0\cdot x$ 所产生的序列 $\underline{a}=(a_j)$ (事实上 $\underline{a}=(a_j)$ 是 $\underline{A}=(A_j)$ 的一个移位序列) 有非零的相关系数 $\rho_i=S_{(f)}(\mu_i,v_0)$, $|\rho_i|>0$, $1\le i\le k$. 从而有

$$P(z_{ij}=a_j)=1/2+\rho_i/2\ne 1/2,\quad 1\le i\le k,\quad j=1,2,\cdots.$$

通过对 $z_i=(z_{ij})$ $(1\le i\le k)$ 作如下变换:

$$c_{ij}=\begin{cases}z_{ij}, & \rho_i=S_{(f)}(\mu_i,v_0)>0;\\ \overline{z}_{ij}=1\oplus z_{ij}, & \rho_i=S_{(f)}(\mu_i,v_0)<0.\end{cases}$$

这样就得到了与 $\underline{a}$ 均有正相关系数的 k 串序列 $c_i=\{c_{ij}: c_{ij}\in F_2,\ j=1,2,3,\cdots\}$, 并且对于 $i=1,2,3,\cdots,k$, 均有 $P(a_j=c_{ij})=1/2+|\rho_i|/2=p_i>1/2$. 因为 $a_j=c_{1j}$, $a_j=c_{2j}$, $\cdots$, $a_j=c_{kj}$ 是相互独立的, 而且 $c_{1j},c_{2j},c_{3j},\cdots,c_{kj}$ 中又仅有 0,1 两种值, 所以我们依据极大似然估计原理, 可以构造出一个序列 e 使其与序列 a 有更大的符合概率. 如何根据这些泄漏的信息设计出有效的算法来构造序列 e 将在下节讨论.

对于 $u \in F_2^m \setminus\{0\}$, 如果存在多个抽头 $x_i \in \{x_1, x_2, \cdots, x_n\}$, 使得 $P(u \cdot f = x_i) = 1/2 + \rho_i/2$, 其中 $\rho_i = S_{(f)}(\mu, v_i)$, $|\rho_i| > 0$, v_i 是第 i 个分量为 1 、其余分量为 0 的 n 维向量. 不妨设 $x_1, x_2, \cdots, x_k, (k \le n)$ 恰是与 $u \cdot f$ 序列有不为 0 的相关系数的 k 个不同抽头. 记 $u \cdot f \triangleq u_1 f_1 \oplus u_2 f_2 \oplus \cdots \bigoplus u_m f_m$ $(u_j \in \mathrm{GF}(2), 1 \le j \le m)$ 产生的序列为 $\underline{b} = \{b_j : b_j \in F_2,\ j = 1, 2, 3, \cdots\}$, 则有 $P(\underline{b} = x_i) = 1/2 + \rho_i/2 \ne 1/2,\ 1 \le i \le k$, 即 $P(b_j = x_{ij}) = 1/2 + \rho_i/2 \ne 1/2,\ 1 \le i \le k,\ j = 1, 2, 3, \cdots$. 再联系到抽头间距的分布规律, 就有 $P(b_j = A_{j+t_i}) = 1/2 + \rho_i/2 \ne 1/2,\ 1 \le i \le k,\ j = 1, 2, 3, \cdots$. 反过来, 亦有 $P(A_j = b_{j-t_i}) = 1/2 + \rho_i/2 \ne 1/2,\ 1 \le i \le k, j \ge t_k$. $\{b_{j-t_i}\}_{j \ge t_k}$, $(1 \le i \le k-1)$ 相当于序列 $\underline{b}$ 截去了前 $t_k - t_i - 1$ 位后剩下的序列, 而 $\{b_{j-t_k}\}_{j \ge t_k}$ 恰是序列 $\underline{b}$. 对 $\{b_{j-t_i}\}_{j \ge t_k}$, $(1 \le i \le k)$ 作如下变换:

$$c_{j-t_i} = \begin{cases} b_{j-t_i}, & \rho_i = S_{(f)}(\mu, e_i) > 0; \\ \bar{b}_{j-t_i} = 1 \oplus b_{j-t_i}, & \rho_i = S_{(f)}(\mu, e_i) < 0. \end{cases}$$

从而得到与序列 $\underline{a}$ 均有正相关系数的 k 串序列 $\{c_{j-t_i}\}_{j \ge t_k}, (1 \le i \le k)$, 并且有 $P(A_j = c_{j-t_i}) = 1/2 + |\rho_i|/2 > 1/2,\ 1 \le i \le k,\ j \ge t_k$. 因为 $A_j = c_j,\ A_j = c_{j-t_2}, \cdots, A_j = c_{j-t_k}$ 可被视作是相互独立的, 且 $c_{j-t_i} \in F_2,\ 1 \le i \le k,\ j \ge t_k$, 所以也可以根据极大似然原理设计出算法来构造一个序列 e 使其与序列 $\underline{A}$ 有较大的符合概率. 如何根据这些泄漏的信息设计出有效的算法来构造序列 e 将在下节讨论.

3　多输出前馈网络的密码分析

上节分两种情况讨论了多输出前馈网络函数的信息泄漏问题. 由讨论过程易知它们实际上可归为下面这种较一般的模型进行研究. 本节我们就在这个一般模型的基础上, 根据极大似然原理设计出一个有效的算法. 用此算法可确定序列 e 使其与序列 $\underline{A}$(或 $\underline{a}$) 有较大的符合概率.

设 $\{a_j\}$ 和 $\{b_{ij}\}$, $(1 \le i \le k)$ 均为 F_2 上的序列, $P(a_j = b_{ij}) = p_i > 1/2,\ i = 1, 2, 3, \cdots, k,\ j = 1, 2, 3, \cdots$; 并设 $a_j = b_{1j}, a_j = b_{2j}, \cdots, a_j = b_{kj}$ 是相互独立的一组关系式. 于是, 由下面给出的算法所构造的序列 $e = \{e_j\}$ 与序列 $\underline{a} = \{a_j\}$ 有较大的符合率.

算法

第一步　选取适当的阈值 $h (h > k/2)$;

第二步　根据 $\{a_j\}$ 和 $\{b_{ij}\}$, $(1 \le i \le k)$ 之间的相关系数, 构造一个序列 $\underline{e} = \{e_j\}$:

$$e_j = \begin{cases} 1, & W_H(r_j) \ge h; \\ 0, & W_H(r_j) \le k - h; \\ b_{rj}, & k - h < W_H(r_j) < h, \end{cases}$$

其中 $W_H(r_j)$ 表示向量 $r_j = \{b_{1j}, b_{2j}, \cdots, b_{kj}\}$ 的汉明重量; r 是使得 $p_r = \max\{p_1, p_2, \cdots, p_k\}$ 成立的最小的下标值.

下面我们将对算法中阈值 h 值的选取、算法的有效性以及符合率 $p(a = e)$ 的估算等问题进行讨论.

对任意固定的 $j, (j = 1, 2, 3, \cdots)$, 我们先考察一下概率 $p(a_j = e_j | r_j)$ 的取值情况:

(1) 当 $k-h<W_H(r_j)<h$ 时，由上述算法，知

$$p(a_j=e_j|r_j)=p_{\max}=\max\{p_1,p_2,\cdots,p_k\}$$

(2) 当 $W_H(r_j)\geq h$ 或 $W_H(r_j)\leq k-h$ 时，设 r_j 中恰有 s 个 b_{ij} 为 $e_j\in \mathrm{GF}(2)$ $(s\geq h)$，不妨设其为 $b_{t_1j},b_{t_2j},\cdots,b_{t_sj}$. 则

$$p(a_j=e_j|r_j)=\frac{p_{t_1}\cdots p_{t_s}(1-p_{t_{s+1}})\cdots(1-p_{t_k})}{p_{t_1}\cdots p_{t_s}(1-p_{t_{s+1}})\cdots(1-p_{t_k})+(1-p_{t_1})\cdots(1-p_{t_s})p_{t_{s+1}}\cdots p_{t_k}}. \tag{1}$$

由此，我们可以进一步来讨论阈值 h 的选取：

假定 $1/2<p_1\leq p_2\leq\cdots\leq p_k<1$ 并且 $k\geq s\geq h>k/2$, 则由上述讨论知：对于任何 $W_H(r_j)=s$ 或 $k-s$ 的 r_j, 均有

$$\begin{aligned}p_j(s)&\triangleq\min_{W_H(r_j)=s\text{或}k-s}P(a_j=e_j|r_j)\\&=\frac{p_1\cdots p_s(1-p_{s+1})\cdots(1-p_k)}{p_1\cdots p_s(1-p_{s+1})\cdots(1-p_k)+(1-p_1)\cdots(1-p_s)p_{s+1}\cdots p_k}\end{aligned} \tag{2}$$

易验证 $p_j(s)$ 是 s 的单调递增函数. 这样若令

$$h=\left[\frac{(k+1)\log p_k/(1-p_k)}{\log p_k/(1-p_k)+\log p_1/(1-p_1)}\right],$$

则可推得对任意的 r_j, 由算法得到的 e_j 与 a_j 的符合率 $p(a_j=e_j|r_j)$ 满足关系式： $p(a_j=e_j|r_j)\geq p_k$ (注：本文中 $[x]$ 表示对 x 进行上取整，即 $[x]$ 是不小于 x 的最小整数) .

根据上述的讨论结果，我们对算法中的 h 值作如下的选取：

令 $p_{\min}\triangleq\min\{p_1,p_2,\cdots,p_k\}$, $p_{\max}\triangleq\max\{p_1,p_2,\cdots,p_k\}$, 则在算法中取定

$$h=\left[\frac{(k+1)\log p_{\max}/(1-p_{\max})}{\log p_{\max}/(1-p_{max})+\log p_{\min}/(1-p_{\min})}\right].$$

特别地，当 $p_1=p_2=\cdots=p_k$ 时，取 $h=[(k+1)/2]$.

由此可见，上面提出的信息收集算法实际上是对密码分析中和编码译码中常常采用的“择多原理”在更一般意义上的推广. 这一推广大大地拓宽了“择多原理”的实际应用背景和范围.

其次，我们来探讨算法的有效性问题.

如果 $h<k$, 则 h 最大只能为 $k-1$ ，因此在 $r_j=(b_{1j},b_{2j},\cdots,b_{r-1,j},b_{rj},b_{r+1,j},\cdots,b_{kj})$ 之中至少当 $b_{1j}=b_{2j}=\cdots=b_{r-1,j}=b_{r+1,j}=\cdots=b_{kj}\neq b_{rj}$ (其中： $\forall r\in\{1,2,\cdots,k\}$) 时，其它 $k-1$ 个信息位能对 b_{rj} 进行纠错. 这说明当 $h<k$ 时，上述算法能够有效地进行纠错，从而可提高输入和输出的符合率. 对上述选取的 h, 欲使 $h<k$, 必须

$$p_{\min}=\frac{(p_{\max}/(1-p_{max}))^{2/(k-1)}}{1+(p_{\max}/(1-p_{\max}))^{2/(k-1)}}.$$

这说明在算法中，选择如上的 h，并使 $p_{\min}$ 符合一定的条件，则算法就能够有效地进行纠错，从而也可有效地提高输入和输出的符合率.

最后，我们来估算序列 a 与 e 的符合率 $p(a=e)$.

前面已讨论了 $p(a_j=e_j|r_j)$ 的分布情况，得知 $p(a_j=e_j|r_j)$ 随着 r_j 的状态的不同而不同. 为了考察 a 与 e 两串序列的符合率，我们可用 $p(a_j=e_j|r_j)$ 的期望值 $E[p(a_j=e_j|r_j)]$ 作为 $p(a=e)$ 的近似值，即可定义：

$$p(a=e)=\lim_{j\to\infty}E[p(a_j=e_j|r_j)].$$

记 r_j 可能出现的所有 2^k 个不同的状态为 $O_1,O_2,O_3,\cdots,O_{2^k}$ (这里： $O_i\in GF(2)^k$, $i=1,2,3,\cdots,2^k$) ， $p(O_i)=p(a_j=e_j|r_j=O_i)$ ，并且假设当 $j\to\infty$ 时， $p(r_j=O_i)\to q_i$, 这样

$$p(a=e)=\sum_{i=1}^{2^k}p(O_i)\cdot q_i. \tag{3}$$

特别地，当 $q_i=1/2^k$ $(i=1,2,3,\cdots,2^k)$ 时，有

$$p(a=e)=\frac{[2^k-2\sum_{i=h}^{k}C_k^i]\times p_{\max}+2\sum_{W_H(O_i)\geq h}p(O_i)}{2^k}. \tag{4}$$

(3), (4) 式表明， $p(a=e)$ 是可以被估算的.

4　多输出 Bent 函数的相关分析

本节我们将针对密码设计中常用到的多输出 Bent 函数作一些探讨.

称 F_2^n 到 F_2^m 上的多输出函数 $f(x)=(f_1,f_2,\cdots,f_m)$ 为多输出 Bent 函数，如果对任意的 $u\in F_2^m\setminus\{0\}$， $u\cdot f$ 均为 Bent 函数.

设 $f(x)$: $F_2^n\to F_2^m$ 为多输出 Bent 函数，则由文献 [5] 中的讨论知，在 $f(x)$ 的 2^{2m} 个不同的输入中，有 $2^{m+1}-1$ 个不同的输入值均对应 $f(x)$ 的输出值 0 ，而 $f(x)$ 的其它 2^m-1 种可能的输出值均对应着 $f(x)$ 的 2^m-1 个不同的输入值. 而且 $p_1=p_2=\cdots=p_m=p$, 因此，利用上节的结果有

$$P(a=e)=\begin{cases}\dfrac{2^m}{2^{2m-1}}\displaystyle\sum_{i=(m+1)/2}^{m}C_m^i\frac{p^i(1-p)^{m-i}}{p^i(1-p)^{m-i}+p^{m-i}(1-p)^i}\\ \quad+\dfrac{1}{2^m}\cdot\dfrac{p^m}{p^m+(1-p)^m}, & m\text{为奇数;}\\ \dfrac{2^m-1}{2^{2m}}\left[C_m^{m/2}p+2\displaystyle\sum_{i=m/2+1}^{m}C_m^i\frac{p^i(1-p)^{m-i}}{p^i(1-p)^{m-i}+p^{m-i}(1-p)^i}\right]\\ \quad+\dfrac{1}{2^m}\cdot\dfrac{p^m}{p^m+(1-p)^m}, & m\text{为偶数.}\end{cases} \tag{6}$$

5 多输出前馈网络信息漏收集算法的应用举例

以一个 "六入三出" 的多输出 Bent 函数为例，来说明应用第 3 节中的算法对多输出变换进行信息漏收集的全过程.

设 f: $F_2^n \to F_2^m$ 为多输出 Bent 函数，并且假设当把 $f(x)$ 表示为 $f(x) = (f_1, f_2, f_3)$ 时，有 $f_1 = x_1x_4 + \oplus x_2x_5 + \oplus x_3x_6 + \oplus x_1 + \oplus x_1x_2x_3$，$f_2 = x_1x_6 + \oplus x_2x_4 + \oplus x_3x_5 + \oplus x_1x_2$，$f_3 = x_1x_5 + \oplus x_2x_6 + \oplus x_3x_4 + \oplus x_2x_3$. 又假定 $f(x)$ 的输入端 x_1, x_2, x_3, x_4, x_5 和 x_6 抽自反馈多项式为 $g(x) = x^{17} + \oplus x_3 + \oplus 1$ 的 17 级线性移存器上，其中 x_1 抽自移存器的第 1 级，x_2 抽自移存器的第 2 级，x_3 抽自移存器的第 4 级，x_4 抽自移存器的第 7 级，x_5 抽自移存器的第 11 级，x_6 抽自移存器的第 16 级 (如图 2 所示) .

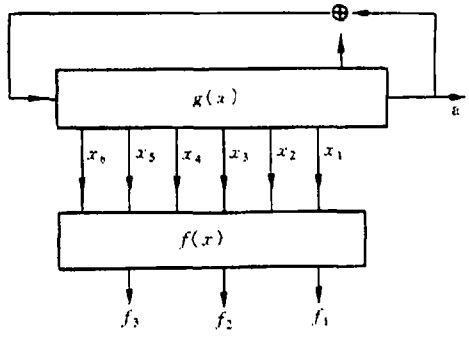

图 2

经过对 $f(x)$ 进行分析，可以得到

$$p(f_i(x) = x_j) = \begin{cases} 0.4375, & \text{当 } i = 1 \text{ 且 } j = 4\text{时;} \\ 0.5625, & \text{其它.} \end{cases}$$

因此，对于 $i = 1, 2, 3$, 有 $p(f_i(x) = x_1) = 0.5625$. 我们在运用算法对本例进行信息漏收集时，就利用一组相关概率均为 0.5625 的三个关系式 $f_1(x) = x_1$ ， $f_2(x) = x_1$ ， $f_3(x) = x_1$ 来进行. 显然，应该有 $h = 2$. 这样，对于我们由算法构造的序列 e, 应有

$$p(x_1 = e) = \frac{2^3 - 1}{2^{2\times 3-1}} \cdot \sum_{i=2}^{3} C_3^i \frac{0.5625^i \times 0.4375^{3-i}}{0.5625^i \times 0.43753^{-i} + 0.5625^{3-i} \times 0.4375^i}$$

$$+ \frac{1}{2^3} \cdot \frac{0.5625^3}{0.5625^3 + 0.4375^3} \approx 0.6029$$

而实际上，我们在实验过程中取得 a 序列的 1851bit, 经与 f_1, f_2, f_3 的输出进行符合统计，有: $p(a = f_1) = 1044/1851 \approx 0.5640$; $p(a = f_2) = 1047/1851 \approx 0.5656$; $p(a = f_3) = 1034/1851 \approx 0.5686$. 而由 f_1, f_2, f_3 的输出序列按算法构造的序列 e', 有 $p(a = e') = 1119/1851 \approx 0.6045$. 可见，理论计算的结果与实验结果是非常接近的，即我们关于概率 $p(a = e)$ 的定义和计算公式是合理的、正确的.

又因为对于 $j=2,3,5,6$ 和 $i=1,2,3$ 也均有 $p(f_i(x)=x_j)=0.5625$, 所以我们可以得到 $p(x_2=e)=p(x_3=e)=p(x_5=e)=p(x_6=e)=p(x_1=e)\approx 0.6029$. 而 x_1,x_2,x_3,x_5,x_6 之间的抽头跨距是不大的，因此，我们还可以进一步在 e 序列上做多输出前馈函数信息漏的收集. 此刻，有 $k=5$, $h=3$. 于是按上面的讨论，我们由算法构造得到的 e'' 序列与 a 序列的符合概率大约为

$$p(a=e'')=\frac{1}{2^5}\times 2\sum_{i=3}^{5}C_5^i\frac{0.6029^i\times 0.3971^{5-i}}{0.6029^i\times 0.3971^{5-i}+0.6029^{5-i}\times 0.3971^i}\approx 0.67547.$$

当 e'' 序列被构造出来后，由于其与多输出网络的输入序列 a 有着更大的符合率，即有 $p(e''=a)>>\max\{p_1,p_2,\cdots,p_k\}$, $i=1,2,3,\cdots$. 这样，若 a 序列的线性反馈多项式已知 (或 a 序列的线性复杂度不高)，我们就可以更容易地利用文献 [2,3,5] 中的方法由 e'' 序列来求出 a 序列的初态 (或 a 序列的产生多项式)，从而实现对该网络系统的攻击.

6 结束语

本文提出了分析多输出前馈网络系统的一种有效算法. 该算法实际上是对密码分析和编码译码中常常采用的“择多原理”在更一般意义上的推广. 实践表明这个算法是非常有效的，它具有很大的实用价值.

参 考 文 献

[1] Siegenthaler T. Crytanalysis representation of nonlinearly filtered ML-sequences, Advances in Cryptology-Eurocrypt'85, LNCS 219. Berlin: spring-Verlag, 1986, 103–110.

[2] Meier W, Staffelbach O. Fast correlation attacks on stream ciphers, Advances in Cryptology-Eurocrypt'88, LNCS 330, Berlin: Springer-Verlag, 1989, 301–314.

[3] Forre'R. A fast correlation attack on nonlinearly feedforward filtered shift-register sequences, Advances in cryptology-Eurocrypt'89, LNCS434, Berlin:Springer-Verlag, 1990, 586–595.

[4] Nyberg K. Perfect nonlinear S-boxes, Advances in Cryptology- Eurocrypt'91, LNCS547, Berlin: Springer-Verlag, 1991, 378–386.

[5] 曾肯成. 密码体制中的熵漏现象. 北京：中国科技大学研究生院 (学术报告). 1987.

CRYPTANALYSIS ON MULTI-OUTPUT FEEDFORWARD NETWORK SYSTEM

Hu Yiping　　Feng Dengguo

(*State Key Lab. of Information Security, Graduate School of Academia Sinica, Beijing* 100039)

Abstract　An algorithm analysing multi-output feedforward network system is discussed in this paper, the basic idea of the algorithm is to collect and utilize information leak of input information at multiple output ends. As an application, a class of important multi-output feedforward network—multi-output Bent functions is analysed by using the algorithm, and the algorithm is illustrated with a concrete example.

Key words　Transformation with multiple-outputs, Majority principie, Bent function, Spectrum, Correlation analysis

胡一平：　男，1963 年生，硕士生，主要从事计算机安全方面的研究工作.

冯登国：　男，1965 年生，研究员，主要从事编码学和密码学方面的教学和科研工作.