复合多输出前馈函数的密码学特性 [1]

陈鲁生 符方伟

(南开大学数学系 天津 300071)

摘 要 该文讨论复合多输出前馈函数和退化的多输出前馈函数，给出了复合多输出前馈函数和退化的多输出前馈函数的一些密码学性质.

关键词 多输出前馈函数，复合函数，退化函数，Resilient 函数，无偏函数，传播准则，线性结构，非线性度

中图号 TN918.1

1 引 言

在前馈网络中，如果选用多输出前馈函数，则可以加快密钥流的生成速度. 因此，对多输出前馈函数的密码学特性进行深入的研究是很有必要的. 文献 [1] 提出了一种多输出前馈函数的相关分析方法. 本文讨论复合多输出前馈函数，它是多输出前馈函数的一种特殊情况，而退化的多输出前馈函数又是复合多输出前馈函数的一种特殊情况. 从目前的文献看来，对退化的单输出前馈函数已进行了比较深入的研究，但对复合多输出前馈函数以及退化的多输出前馈函数，据我们所知，似乎还没有进行过深入的研究. 本文讨论复合多输出前馈函数以及退化的多输出前馈函数的密码学特性，得到了一些有意义的结果.

2 基本概念和记号

设 V_n =GF(2)^n 是二元域上的 n 维向量空间. 对任意 $\alpha \in V_n$, $W(\alpha)$ 表示 α 的 Hamming 重量，即向量 α 的分量中 1 的个数.

多输出前馈函数实际上就是从 V_n 到 V_m 的函数. 设 $\mathcal{F}_{n,m}$ 是所有从 V_n 到 V_m 的函数的集合. 对任意 $F \in \mathcal{F}_{n,m}$, F 可以表示为 $F=(f_1, f_2, \ldots, f_m)$, 其中每个分量函数 f_i, $1 \le i \le m$, 都是 V_n 上的函数，即 $f_i \in \mathcal{F}_{n,1}$. 设 NLC_F 是 F 的分量函数的所有非零线性组合的集合.

设 $f \in \mathcal{F}_{n,1}$, f 可以表示成变量乘积的和，其中最长乘积项中变量的个数称为 f 的代数次数，记为 $\deg(f)$. 若 f 的形式为 $f(x)=c_0 \oplus c_1 x_1 \oplus \cdots \oplus c_n x_n$, $c_i \in$GF(2), $0 \le i \le n$, 则称 f 是仿射函数. V_n 上的两个函数 f 与 g 的 Hamming 距离定义为 $d(f,g) \stackrel{\mathrm{def}}{=} \sum_{x \in V_n} f(x) \oplus g(x)$. f 的非线性度定义为 $N_f \stackrel{\mathrm{def}}{=} \min_{\varphi \in \mathrm{AF}_n} d(f, \varphi)$, 其中 AF_n 表示 V_n 上的所有仿射函数的集合.

我们用 $[n,k,d]$ 表示极小距离为 d, 长为 n 的 k 维线性码，它是 V_n 的一个 k 维子空间. 一个 $[n,k,d]$ 线性码 C 的生成矩阵 A 是 GF(2) 上的 $k \times n$ 阶矩阵，$\mathrm{Rank}(A)=k$, 其行向量是 C 的一组基.

3 退化的多输出前馈函数

定义 1 设 $F \in \mathcal{F}_{n,m}$. 如果存在 $G \in \mathcal{F}_{k,m}$ 和 $H \in \mathcal{F}_{n,k}$, 并且 $k < n$, 使得对任意 $x \in V_n$, $F(x)=G(H(x))$, 则称 F 是复合函数.

[1] 1999-04-05 收到，1999-10-06 定稿
国家自然科学基金资助项目，批准号：69802008

定义 2　设 $F \in \mathcal{F}_{n,m}$. 如果存在 $G \in \mathcal{F}_{k,m}$ 和 GF(2) 上的 $n \times k$ 阶矩阵 D, $k < n$, $\mathrm{Rank}(D) = k$, 使得对任意 $x \in V_n$, $F(x) = G(xD)$, 则称 F 可退化为 G, 简称 F 是退化的, 否则称 F 是非退化的.

定义 3　设 $F \in \mathcal{F}_{n,m}$. $AD(F) \stackrel{\mathrm{def}}{=} n - \min\{\, k \mid k < n,$ 存在$G \in \mathcal{F}_{k,m}$, F可退化为$G \,\}$, 称为 F 的退化度. 若 F 是非退化的, 则令 $AD(F) = 0$.

记号 1　设 $F \in \mathcal{F}_{n,m}$. $DM(F) \stackrel{\mathrm{def}}{=} \{\, D \mid D$是GF(2)上的$n \times k$阶矩阵, $k < n$,$\mathrm{Rank}(D) = k$, 并且存在$G \in \mathcal{F}_{k,m}$, 使得对任意$x \in V_n, F(x) = G(xD) \,\}$.

定理 1　设 $F = (f_1, f_2, \ldots, f_m) \in \mathcal{F}_{n,m}$, 则 $DM(F) = \bigcap_{i=1}^{m} DM(f_i)$.

证明　设 D 是 GF(2) 上的 $n \times k$ 阶矩阵, $k < n$, $\mathrm{Rank}(D) = k$, 则 $D \in DM(F) \iff$ 存在 $G = (g_1, g_2, \ldots, g_m) \in \mathcal{F}_{k,m}$, 使得对任意 $x \in V_n$, $F(x) = G(xD) \iff$ 对任意 $1 \le i \le m$, 存在 $g_i \in \mathcal{F}_{k,1}$, 使得对任意 $x \in V_n$, $f_i(x) = g_i(xD) \iff$ 对任意 $1 \le i \le m$, $D \in DM(f_i)$ $\iff D \in \bigcap_{i=1}^{m} DM(f_i)$. 因此, $DM(F) = \bigcap_{i=1}^{m} DM(f_i)$.　证毕

推论 1　$F = (f_1, f_2, \ldots, f_m) \in \mathcal{F}_{n,m}$ 是退化的 $\iff \bigcap_{i=1}^{m} DM(f_i) \neq \emptyset$.

推论 2　设 $F = (f_1, f_2, \ldots, f_m) \in \mathcal{F}_{n,m}$, 则 $AD(F) = n - \min\{\, k \mid$ 存在$D_{n\times k} \in \bigcap_{i=1}^{m} DM(f_i) \,\}$.

定理 2　设 $F = (f_1, f_2, \ldots, f_m) \in \mathcal{F}_{n,m}$ 是复合函数, 则 $f_1, f_2, \ldots, f_m$ 的任意非零线性组合都是复合函数.

证明　设 $F = (f_1, f_2, \ldots, f_m) \in \mathcal{F}_{n,m}$ 是复合函数, 则存在 $G = (g_1, g_2, \ldots, g_m) \in \mathcal{F}_{k,m}$ 和 $H \in \mathcal{F}_{n,k}$, 使得对任意 $x \in V_n$, $F(x) = G(H(x))$. 因此, 对任意 $1 \le i \le m$, $f_i(x) = g_i(H(x))$. 设 $f(x) = \bigoplus_{i=1}^{m} c_i f_i(x)$ 是 F 的分量函数的任意非零线性组合, $g(y) = \bigoplus_{i=1}^{m} c_i g_i(y)$ 是 G 的分量函数的任意非零线性组合, 其中 $c_i \in$GF(2), $1 \le i \le m$. 则 $f(x) = \bigoplus_{i=1}^{m} c_i f_i(x) = \bigoplus_{i=1}^{m} c_i g_i(H(x)) = g(H(x))$. 因此, $f_1, f_2, \ldots, f_m$ 的任意非零线性组合都是复合函数. 证毕

因为退化的多输出前馈函数是复合多输出前馈函数的特例, 所以采用与定理 2 的证明类似的方法, 可以证明下述定理 3 成立.

定理 3　设 $F = (f_1, f_2, \ldots, f_m) \in \mathcal{F}_{n,m}$ 是退化的, 则 $f_1, f_2, \ldots, f_m$ 的任意非零线性组合都是退化的.

需要指出的是定理 2 和定理 3 的逆命题不成立.

例 1　设 $F(x_1, x_2, x_3, x_4) = (f_1(x_1, x_2, x_3, x_4), f_2(x_1, x_2, x_3, x_4))$, 其中 $f_1(x_1, x_2, x_3, x_4) = x_1x_2 \oplus x_1x_3$, $f_2(x_1, x_2, x_3, x_4) = x_2x_3 \oplus x_3x_4 \oplus x_1x_4$.

设

$$g_1(y_1, y_2) = y_1y_2, \quad H_1(x_1, x_2, x_3, x_4) = (x_1, x_2 \oplus x_3)$$

$$g_2(y_1, y_2, y_3) = y_1 \oplus y_2y_3, \quad H_2(x_1, x_2, x_3, x_4) = (x_1x_2, x_1 \oplus x_3, x_2 \oplus x_4)$$

$$g_3(y_1, y_2, y_3) = y_1 \oplus y_2y_3, \quad H_3(x_1, x_2, x_3, x_4) = (x_1x_3, x_1 \oplus x_3, x_2 \oplus x_4)$$

则

$$f_1(x_1, x_2, x_3, x_4) = x_1(x_2 \oplus x_3) = g_1(H_1(x_1, x_2, x_3, x_4))$$

$$f_2(x_1, x_2, x_3, x_4) = x_1x_2 \oplus (x_1 \oplus x_3)(x_2 \oplus x_4) = g_2(H_2(x_1, x_2, x_3, x_4))$$

$$f_1(x_1, x_2, x_3, x_4) \oplus f_2(x_1, x_2, x_3, x_4) = x_1x_3 \oplus (x_1 \oplus x_3)(x_2 \oplus x_4) = g_3(H_3(x_1, x_2, x_3, x_4))$$

因此， $F(x_1,x_2,x_3,x_4)$ 的分量函数的每一个非零线性组合都是复合函数. 但是，容易证明 $F(x_1,x_2,x_3,x_4)$ 不是复合函数.

例 2 设 $F(x_1,x_2,x_3,x_4)=(f_1(x_1,x_2,x_3,x_4),f_2(x_1,x_2,x_3,x_4))$, 其中 $f_1(x_1,x_2,x_3,x_4)=x_1x_2\oplus x_4$, $f_2(x_1,x_2,x_3,x_4)=x_2x_3\oplus x_4$.

设 $g_1(y_1,y_2,y_3)=y_1y_2\oplus y_3$, $g_2(y_1,y_2)=y_1y_2$. 容易证明 $g_1(y_1,y_2,y_3)$ 和 $g_2(y_1,y_2)$ 都是非退化函数.

设

$$D_1=\begin{pmatrix}1&0&0\\0&1&0\\0&0&0\\0&0&1\end{pmatrix},\quad D_2=\begin{pmatrix}0&0&0\\1&0&0\\0&1&0\\0&0&1\end{pmatrix},\quad D_3=\begin{pmatrix}0&1\\1&0\\0&1\\0&0\end{pmatrix}$$

则

$$f_1(x_1,x_2,x_3,x_4)=x_1x_2\oplus x_4=g_1((x_1,x_2,x_3,x_4)D_1)$$

$$f_2(x_1,x_2,x_3,x_4)=x_2x_3\oplus x_4=g_1((x_1,x_2,x_3,x_4)D_2)$$

$$f_1(x_1,x_2,x_3,x_4)\oplus f_2(x_1,x_2,x_3,x_4)=x_1x_2\oplus x_2x_3=g_2((x_1,x_2,x_3,x_4)D_3)$$

因此， $F(x_1,x_2,x_3,x_4)$ 的分量函数的每一个非零线性组合都是退化的. 但是，容易证明 $F(x_1,x_2,x_3,x_4)$ 是非退化的.

4 复合多输出前馈函数的密码学性质

4.1 Resilient 函数

定义 4 设 $n\ge m\ge 1$, $F\in\mathcal{F}_{n,m}$, $t\ge 0$, $T=\{j_1,j_2,\ldots,j_t\}\subseteq\{1,2,\ldots,n\}$. 如果对任意 $(a_1,a_2,\ldots,a_t)\in V_t$ 和任意 $\beta\in V_m$,

$$|\{x\mid x=(x_1,x_2,\ldots,x_n)\in V_n,\ x_{j_1}=a_1,x_{j_2}=a_2,\ldots,x_{j_t}=a_t,\ F(x)=\beta\}|=2^{n-m-t}$$

则称 F 关于 T 是无偏的. 当 $t=0$ 时，也就是说，如果对任意 $\beta\in V_m$,

$$|\{x\mid x\in V_n,\ F(x)=\beta\}|=2^{n-m}$$

则称 F 是无偏的.

定义 5 设 $n\ge m\ge 1$, $F\in\mathcal{F}_{n,m}$, $t\ge 0$. 如果 F 关于 $\{1,2,\ldots,n\}$ 的每一个子集 T 是无偏的，这里 $|T|=t$, 则称 F 是 (n,m,t)-resilient 函数.

定理 4 设 H 是 (n,m,t)-resilient 函数， $G\in\mathcal{F}_{m,s}$ 是无偏函数，则 $F(x)=G(H(x))$ 是 (n,s,t)-resilient 函数.

证明 因为 H 是 (n,m,t)-resilient 函数，所以对任意的 $\{j_1,j_2,\ldots,j_t\}\subseteq\{1,2,\ldots,n\}$ 和 $(a_1,a_2,\ldots,a_t)\in V_t$ 以及 $\alpha\in V_m$,

$$|\{x\mid x=(x_1,x_2,\ldots,x_n)\in V_n,\ x_{j_1}=a_1,x_{j_2}=a_2,\ldots,x_{j_t}=a_t,\ H(x)=\alpha\}|=2^{n-m-t}$$

又因为 $G\in\mathcal{F}_{m,s}$ 是无偏函数，所以对任意的 $\beta\in V_s$,

$$|\{\alpha\mid\alpha\in V_m,\ G(\alpha)=\beta\}|=2^{m-s}$$

因此，对任意的 $\{j_1, j_2, \ldots, j_t\} \subseteq \{1, 2, \ldots, n\}$ 和 $(a_1, a_2, \ldots, a_t) \in V_t$ 以及 $\beta \in V_s$，

$$\begin{aligned}
&|\{x \mid x = (x_1, x_2, \ldots, x_n) \in V_n,\ x_{j_1} = a_1, x_{j_2} = a_2, \ldots, x_{j_t} = a_t,\ G(H(x)) = \beta\}| \\
&= \sum_{\alpha \in G^{-1}(\beta)} |\{x \mid x = (x_1, x_2, \ldots, x_n) \in V_n,\ x_{j_1} = a_1, x_{j_2} = a_2, \ldots, x_{j_t} = a_t,\ H(x) = \alpha\}| \\
&= 2^{n-m-t}|G^{-1}(\beta)| \\
&= 2^{n-m-t}2^{m-s} = 2^{n-s-t}
\end{aligned}$$

所以 $F(x) = G(H(x))$ 是 (n, s, t)-resilient 函数. 证毕

引理 1[2]　设 D^T 是一个 $[n, k, d]$ 线性码的生成矩阵，则 $H(x) = xD$ 是 $(n, k, d-1)$-resilient 函数.

由定理 4 和引理 1，我们得到下述结论.

推论 3　设 D^T 是一个 $[n, k, d]$ 线性码的生成矩阵，$G \in \mathcal{F}_{k,m}$ 是无偏函数，则 $F(x) = G(xD)$ 是 $(n, m, d-1)$-resilient 函数.

引理 2[3]　$F = (f_1, f_2, \ldots, f_m) \in \mathcal{F}_{n,m}$ 是 (n, m, t)-resilient 函数 $\Longleftrightarrow$ $f_1, f_2, \ldots, f_m$ 的每一个非零线性组合 $f(x) = \bigoplus_{i=1}^{m} c_i f_i(x)$ 都是 $(n, 1, t)$-resilient 函数，其中 $x \in V_n$.

引理 3　设 $H = (h_1, h_2, \ldots, h_m) \in \mathcal{F}_{n,m}$ 是 (n, m, t)-resilient 函数，D 是 GF(2) 上的 $m \times k$ 阶矩阵，$k \leq m$, $\mathrm{Rank}(D) = k$，则 $F(x) = H(x)D = (h_1(x), h_2(x), \ldots, h_m(x))D$ 是一个 (n, k, t)-resilient 函数，其中 $x \in V_n$.

证明　对任意的 $0 \neq \beta \in V_k$，设 $f(x) = F(x)\beta^T$ 是 $F(x)$ 的分量函数的任意非零线性组合. $f(x) = F(x)\beta^T = H(x)D\beta^T = H(x)(\beta D^T)^T$. 因为 $\mathrm{Rank}(D) = k$，所以 βD^T 是 V_m 中的非零向量. 因此，$f(x)$ 是 $H(x)$ 的分量函数的非零线性组合，所以根据引理 2 知，$f(x)$ 是 $(n, 1, t)$-resilient 函数. 再根据引理 2 知，$F(x)$ 是 (n, k, t)-resilient 函数. 证毕

引理 3 和定理 4 实际上提供了两种构造 resilient 函数的方法. 由引理 3 和定理 4，我们立即得到下述推论.

推论 4　设 $H = (h_1, h_2, \ldots, h_m) \in \mathcal{F}_{n,m}$ 是 (n, m, t)-resilient 函数，D 是 GF(2) 上的 $m \times k$ 阶矩阵，$k \leq m$, $\mathrm{Rank}(D) = k$, $G \in \mathcal{F}_{k,s}$ 是无偏函数，则 $F(x) = G(H(x)D)$ 是 (n, s, t)-resilient 函数，其中 $x \in V_n$.

4.2 无偏函数

定理 5　设 $H \in \mathcal{F}_{n,k}$ 是无偏函数，$n \geq k$. 设 $G \in \mathcal{F}_{k,m}$, $F \in \mathcal{F}_{n,m}$，并且对任意 $x \in V_n$, $F(x) = G(H(x))$，则对任意 $\alpha \in V_m$，

$$|\{x \in V_n \mid F(x) = \alpha\}| = 2^{n-k}|\{y \in V_k \mid G(y) = \alpha\}|$$

特别地，F 是无偏函数 $\Longleftrightarrow$ G 是无偏函数.

证明　因为 H 是无偏函数，所以对任意 $y \in V_k$，

$$|\{x \in V_n \mid H(x) = y\}| = 2^{n-k}$$

因此，对任意 $\alpha \in V_m$，

$$\begin{aligned}|\{x \in V_n \mid F(x)=\alpha\}| &= |\{x \in V_n \mid G(H(x))=\alpha\}| \\ &= \sum_{y \in G^{-1}(\alpha)} |\{x \in V_n \mid H(x)=y\}| \\ &= 2^{n-k}|G^{-1}(\alpha)| \\ &= 2^{n-k}|\{y \in V_k \mid G(y)=\alpha\}|\end{aligned}$$

由上式可以看出，对任意 $\alpha \in V_m$，$|\{x \in V_n \mid F(x)=\alpha\}|=2^{n-m} \iff |\{y \in V_k \mid G(y)=\alpha\}|=2^{k-m}$．所以，$F$ 是无偏函数 $\iff$ G 是无偏函数． 证毕

推论 5 设 $F \in \mathcal{F}_{n,m}, G \in \mathcal{F}_{k,m}, n \geq k$．设 D 是 GF(2) 上的 $n \times k$ 阶矩阵，$\mathrm{Rank}(D)=k$，并且对任意 $x \in V_n$，$F(x)=G(xD)$，则对任意 $\alpha \in V_m$，

$$|\{x \in V_n \mid F(x)=\alpha\}|=2^{n-k}|\{y \in V_k \mid G(y)=\alpha\}|$$

特别地，F 是无偏函数 $\iff$ G 是无偏函数．

证明 设 $H(x)=xD$，则根据引理 1 和 resilient 函数的定义可知 H 是无偏函数．因此，由定理 5 知结论成立． 证毕

4.3 传播准则

定义 6 设 $F \in \mathcal{F}_{n,m}, n \geq m$．如果对任意满足 $1 \leq W(\alpha) \leq k$ 的 $\alpha \in V_n$，$F(x) \oplus F(x \oplus \alpha)$ 是无偏函数，则称 F 满足 k 阶传播准则．

定理 6 设 $F \in \mathcal{F}_{n,m}, G \in \mathcal{F}_{k,m}, n \geq k \geq m$．设 D 是 GF(2) 上的 $n \times k$ 阶矩阵，$\mathrm{Rank}(D)=k$，并且对任意 $x \in V_n$，$F(x)=G(xD)$．设 G 满足 t 阶传播准则，$t \leq k$．如果对任意满足 $1 \leq W(\alpha) \leq s$ 的 $\alpha \in V_n$，$1 \leq W(\alpha D) \leq t$，则 F 满足 s 阶传播准则．

证明 因为对任意满足 $1 \leq W(\alpha) \leq s$ 的 $\alpha \in V_n$，$1 \leq W(\alpha D) \leq t$，并且 G 满足 t 阶传播准则，所以根据传播准则的定义和推论 5 知，$F(x) \oplus F(x \oplus \alpha)=G(xD) \oplus G(xD \oplus \alpha D)$ 是无偏函数．因此，F 满足 s 阶传播准则． 证毕

应该注意传播准则不一定是可继承的，也就是说，如果 $F(x)=G(xD)$，则 G 满足传播准则不能保证 F 也满足传播准则．

例 3 设

$$D=\begin{pmatrix}1 & 1 & 1\\ 1 & 1 & 0\\ 0 & 1 & 1\\ 1 & 0 & 1\end{pmatrix}$$

$g(y_1,y_2,y_3)=1 \oplus y_1 \oplus y_1y_2 \oplus y_1y_3 \oplus y_2y_3$．容易验证 g 满足 2 阶传播准则，但是，$f(x_1,x_2,x_3,x_4)=g((x_1,x_2,x_3,x_4)D)=1 \oplus x_3 \oplus x_2x_3 \oplus x_2x_4 \oplus x_3x_4$ 不满足任何阶的传播准则．

推论 6 设 $F \in \mathcal{F}_{n,m}, G \in \mathcal{F}_{k,m}, n \geq k \geq m$．设 D 是 GF(2) 上的 $n \times k$ 阶矩阵，$\mathrm{Rank}(D)=k$，并且对任意 $x \in V_n$，$F(x)=G(xD)$．设对任意满足 $1 \leq W(\alpha) \leq s$ 的 $\alpha \in V_n$，$W(\alpha D)>0$，并且存在满足 $W(\beta)=s+1$ 的 $\beta \in V_n$，使得 $W(\beta D)=0$．如果 G 满足 k 阶传播准则，则 F 满足 s 阶传播准则，并且 F 不满足 $s+1$ 阶传播准则．

证明 因为 D 是 GF(2) 上的 $n \times k$ 阶矩阵，并且对任意满足 $1 \leq W(\alpha) \leq s$ 的 $\alpha \in V_n$，$W(\alpha D)>0$，所以对任意满足 $1 \leq W(\alpha) \leq s$ 的 $\alpha \in V_n$，$1 \leq W(\alpha D) \leq k$．又因为 G 满足 k 阶传播准则，所以，根据定理 6 知，F 满足 s 阶传播准则．

另一方面，因为存在满足 $W(\beta)=s+1$ 的 $\beta\in V_n$，使得 $W(\beta D)=0$，所以 $F(x)\oplus F(x\oplus\beta)=G(xD)\oplus G(xD\oplus\beta D)=G(xD)\oplus G(xD)=0$．因此，$F$ 不满足 $s+1$ 阶传播准则．　证毕

4.4 线性结构

定义 7　设 $F\in\mathcal{F}_{n,m}$，$\alpha\in V_n$．如果存在 $\beta\in V_m$，使得对任意 $x\in V_n$，$F(x)\oplus F(x\oplus\alpha)=\beta$，则称 α 是 F 的线性结构．

定理 7　设 $H\in\mathcal{F}_{n,k}$，对任意 $y\in V_k$，$|\{x\in V_n\mid H(x)=y\}|\geq 1$．设 $G\in\mathcal{F}_{k,m}$，$F\in\mathcal{F}_{n,m}$，对任意 $x\in V_n$，$F(x)=G(H(x))$．设 $\alpha\in V_n$ 是 H 的线性结构，则 α 是 F 的线性结构 $\Longleftrightarrow$ $H(\alpha)\oplus H(0)$ 是 G 的线性结构．

证明　因为 α 是 H 的线性结构，所以存在 $\beta\in V_k$，使得对任意 $x\in V_n$，$H(x)\oplus H(x\oplus\alpha)=\beta$．取 $x=0$，可知 $\beta=H(\alpha)\oplus H(0)$．

如果 $H(\alpha)\oplus H(0)$ 是 G 的线性结构，则存在 $\beta_1\in V_m$，使得对任意 $y\in V_k$，$G(y)\oplus G(y\oplus H(\alpha)\oplus H(0))=\beta_1$．因此，对任意 $x\in V_n$，$F(x)\oplus F(x\oplus\alpha)=G(H(x))\oplus G(H(x\oplus\alpha))=G(H(x))\oplus G(H(x)\oplus H(\alpha)\oplus H(0))=\beta_1$，所以 α 是 F 的线性结构．

反过来，如果 α 是 F 的线性结构，则存在 $\beta_2\in V_m$，使得对任意 $x\in V_n$，$F(x)\oplus F(x\oplus\alpha)=\beta_2$．因此，$G(H(x))\oplus G(H(x)\oplus H(\alpha)\oplus H(0))=G(H(x))\oplus G(H(x\oplus\alpha))=F(x)\oplus F(x\oplus\alpha)=\beta_2$．令 $y=H(x)$．因为对任意 $y\in V_k$，$|\{x\in V_n\mid H(x)=y\}|\geq 1$，所以当 x 取遍 V_n 中的所有向量时，y 也取遍 V_k 中的所有向量．因此，$G(y)\oplus G(y\oplus H(\alpha)\oplus H(0))=\beta_2$．所以 $H(\alpha)\oplus H(0)$ 是 G 的线性结构．　证毕

推论 7　设 $F\in\mathcal{F}_{n,m}$，$G\in\mathcal{F}_{k,m}$，$n\geq k$．设 D 是 GF(2) 上的 $n\times k$ 阶矩阵，$\mathrm{Rank}(D)=k$，并且对任意 $x\in V_n$，$F(x)=G(xD)$．设 $\alpha\in V_n$，则 α 是 F 的线性结构 $\Longleftrightarrow$ αD 是 G 的线性结构．

记号 2　设 $F\in\mathcal{F}_{n,m}$，$E^{(F)}$ 表示 F 的所有线性结构的集合．

推论 8　设 $F\in\mathcal{F}_{n,m}$，$G\in\mathcal{F}_{k,m}$，$n\geq k$．设 D 是 GF(2) 上的 $n\times k$ 阶矩阵，$\mathrm{Rank}(D)=k$，并且对任意 $x\in V_n$，$F(x)=G(xD)$，则 $|E^{(F)}|=2^{n-k}|E^{(G)}|$．

证明　设 $\beta\in V_k$ 是 G 的一个线性结构，则根据推论 7 知，方程 $xD=\beta$ 的每一个解都是 F 的线性结构．因为 $\mathrm{Rank}(D)=k$，所以方程 $xD=\beta$ 有 2^{n-k} 个解．因此，$|E^{(F)}|=2^{n-k}|E^{(G)}|$．　证毕

由推论 8 可以看出，即使 G 没有非零的线性结构，F 也会有非零的线性结构，并且当 F 的退化度越大时，F 的线性结构也越多．从这一方面来看，退化的多输出前馈函数在密码学上似乎是安全性较弱的函数．

4.5 非线性度与代数次数

定义 8　设 $F\in\mathcal{F}_{n,m}$，$N_F\stackrel{\mathrm{def}}{=}\min_{f\in\mathrm{NLC}_F}N_f$，称为 F 的非线性度．

定义 9　设 $F\in\mathcal{F}_{n,m}$，$\deg(F)\stackrel{\mathrm{def}}{=}\min_{f\in\mathrm{NLC}_F}\deg(f)$，称为 F 的代数次数．

引理 4[3]　设 $f\in\mathcal{F}_{n,1}$，$g\in\mathcal{F}_{k,1}$，$n\geq k$．设 D 是 GF(2) 上的 $n\times k$ 阶矩阵，$\mathrm{Rank}(D)=k$，并且对任意 $x\in V_n$，$f(x)=g(xD)$，则 $N_f=2^{n-k}N_g$，$\deg(f)=\deg(g)$．

定理 8　设 $F\in\mathcal{F}_{n,m}$，$G\in\mathcal{F}_{k,m}$，$n\geq k$．设 D 是 GF(2) 上的 $n\times k$ 阶矩阵，$\mathrm{Rank}(D)=k$，并且对任意 $x\in V_n$，$F(x)=G(xD)$，则 $N_F=2^{n-k}N_G$，$\deg(F)=\deg(G)$．

证明　设 $F=(f_1,f_2,\ldots,f_m)$，$G=(g_1,g_2,\ldots,g_m)$．设 $f(x)=\bigoplus_{i=1}^m c_if_i(x)$ 是 F 的分量函数的任意非零线性组合，$g(y)=\bigoplus_{i=1}^m c_ig_i(y)$ 是 G 的分量函数的任意非零线性组合，其中 $c_i\in\mathrm{GF}(2)$，$1\leq i\leq m$．因为 $F(x)=G(xD)$，所以 $f_i(x)=g_i(xD)$，$1\leq i\leq m$．

因此， $f(x)=\bigoplus_{i=1}^{m}c_if_i(x)=\bigoplus_{i=1}^{m}c_ig_i(xD)=g(xD)$. 根据引理 4 知， $N_f=2^{n-k}N_g$, $\deg(f)=\deg(g)$. 因此，根据多输出前馈函数的非线性度和代数次数的定义知，

$$\begin{aligned}N_F&=\min_{(0,0,\ldots,0)\neq(c_1,c_2,\ldots,c_m)\in V_m}N_f\\&=\min_{(0,0,\ldots,0)\neq(c_1,c_2,\ldots,c_m)\in V_m}2^{n-k}N_g\\&=2^{n-k}\min_{(0,0,\ldots,0)\neq(c_1,c_2,\ldots,c_m)\in V_m}N_g\\&=2^{n-k}N_G\\\deg(F)&=\min_{(0,0,\ldots,0)\neq(c_1,c_2,\ldots,c_m)\in V_m}\deg(f)\\&=\min_{(0,0,\ldots,0)\neq(c_1,c_2,\ldots,c_m)\in V_m}\deg(g)\\&=\deg(G)\end{aligned}$$

证毕

例 4 设 $G(y_1,y_2,y_3)=(y_2\oplus y_1y_3,1\oplus y_1\oplus y_2\oplus y_3\oplus y_2y_3)$. 设 $g_1(y_1,y_2,y_3)=y_2\oplus y_1y_3$, $g_2(y_1,y_2,y_3)=1\oplus y_1\oplus y_2\oplus y_3\oplus y_2y_3$, $g_3(y_1,y_2,y_3)=g_1(y_1,y_2,y_3)\oplus g_2(y_1,y_2,y_3)=1\oplus y_1\oplus y_3\oplus y_1y_3\oplus y_2y_3$. 容易验证 $N_{g_1}=2$, $N_{g_2}=2$, $N_{g_3}=2$. 因此， $N_G=2$.

设

$$D=\begin{pmatrix}1&0&1\\1&0&0\\1&1&0\\0&1&0\\0&1&1\\0&0&1\end{pmatrix}$$

$F(x)=G(xD)=(f_1(x),f_2(x))$, 其中

$$x=(x_1,x_2,x_3,x_4,x_5,x_6)$$

$$f_1(x)=x_1\oplus x_3\oplus x_4\oplus x_5\oplus x_1x_2\oplus x_1x_3\oplus x_1x_5\oplus x_1x_6\oplus x_2x_5\oplus x_2x_6\oplus x_3x_5\oplus x_3x_6$$

$$f_2(x)=1\oplus x_2\oplus x_4\oplus x_5\oplus x_6\oplus x_1x_3\oplus x_1x_4\oplus x_1x_5\oplus x_3x_5\oplus x_3x_6\oplus x_4x_5\oplus x_4x_6\oplus x_5x_6$$

根据定理 8 知， $N_F=2^{6-3}N_G=16$, $\deg(F)=\deg(G)$.

进一步，容易验证 G 是无偏函数，并且 G 不是 $(3,2,1)$-resilient 函数. 另外，由 D^T 生成的线性码的极小距离 $d=3$. 根据引理 1 知

$$\begin{aligned}H(x_1,x_2,x_3,x_4,x_5,x_6)&=(x_1,x_2,x_3,x_4,x_5,x_6)D\\&=(x_1\oplus x_2\oplus x_3,x_3\oplus x_4\oplus x_5,x_5\oplus x_6\oplus x_1)\end{aligned}$$

是 $(6,3,2)$-resilient 函数. 由推论 3 知， $F(x)=G(xD)$ 是 $(6,2,2)$-resilient 函数.

从例 4 可以看出退化的多输出前馈函数除了具有线性结构外，其它的密码学特性还是比较好的.

5 结束语

本文讨论了复合多输出前馈函数以及退化的多输出前馈函数的密码学特性，给出了一些在理论和应用上都有一定意义的结果. 尽管退化的多输出前馈函数具有较多的线性结构，并

且当其退化度越大时，线性结构越多，而线性结构越多，其可能达到的最大非线性度越小[4]，但是，从定理 8 可以看出，退化的多输出前馈函数 $F(x)=G(xD)$ 的非线性度比 G 的非线性度高得多．另一方面，如果 G 是无偏函数，则可以适当地选取矩阵 D，使得 $F(x)=G(xD)$ 是具有较高阶的 resilient 函数．进一步，如果函数 G 和矩阵 D 选取适当，还可以使 $F(x)=G(xD)$ 满足传播准则．因此，退化的多输出前馈函数仍然具有一定的密码学意义．当然，在实际设计密码体制时，还是应该尽量选用非退化的或退化度较小的多输出前馈函数，以免其具有过多的线性结构．对于一般的复合多输出前馈函数 $F(x)=G(H(x))$，如果 H 和 G 选取适当，则也可以使 F 具有较好的密码学性质．

参 考 文 献

[1] 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.

[2] Bennett C H, Brassard G, Robert J M. Privacy amplification by public discussion. SIAM J. Comput., 1988, 17(2): 210–229.

[3] Zhang X M, Zheng Y. Cryptographically resilient functions. IEEE Trans. Inform. Theory, 1997, 43(5): 1740–1747.

[4] 冯登国，肖国镇．布尔函数的对偶性和线性点．通信学报，1996, 17(1): 46–50.

CRYPTOGRAPHIC PROPERTIES OF COMPOSITE MULTI-OUTPUT FEEDFORWARD FUNCTIONS

Chen Lusheng　　Fu Fangwei

(*Department of Mathematics, Nankai University, Tianjin* 300071)

Abstract　In this paper, composite and degenerated multi-output feedforward functions are discussed and some cryptographic properties of them are given.

Key words　Multi-output feedforward function, Composite function, Degenerated function, Resilient function, Unbiased function, Propagation criterion, Linear structure, Nonlinearity

陈鲁生：　男，1962 年生，副教授，主要从事密码学和应用数学等方面的研究．

符方伟：　男，1963 年生，教授，主要从事信息论和编码以及密码学等方面的研究．