第 13 卷 第 3 期　　电 子 科 学 学 刊　　Vol. 13, No. 3
1991 年 5 月　　JOURNAL OF ELECTRONICS　　May, 1991

抗熵漏前馈网络研究*

杨义先　　胡正名
（北京邮电学院，北京）

摘要　本文从实际出发减弱了 Siegenthaler 的“相关免疫”限制条件，实现了在不作出实质性“牺牲”的前提下避免了相关免疫性与线性复杂度之间的折衷（trade-off）. 接着将 Bent 函数引入前馈网络的线性逼近熵漏现象的研究之中，得出了一些新结果. 文中的研究方法也与前人不同.

关键词　密码；前馈网络；相关免疫；抗熵漏

一、引　言

前馈网络是一类非常重要的密钥流生成器. 但是与别的密钥流生成器一样，前馈网络也有其弱点. 例如 Sigenthaler[1-3] 发现，如果网络函数 $f(x_1,\cdots,x_n)$ 的“相关免疫性”很差，那么相应的流密码体系就可被相关攻击法破译. 为此前人引入了“m 阶相关免疫”的概念. 但后来人们发现，若按上述“相关免疫”要求来设计前馈网络时，会出现这样一个矛盾，即相关免疫性越好，其输出密钥流的线性复杂度就越差. 可见相关免疫性的加强是以“牺牲”线性复杂度为代价的. 这显然不能令人满意，因为线性复杂度也是密码安全度的一个重要指标. 为克服上述矛盾，前人通过增加设备和成本作了不少努力[4]. 而本文第二节将以全新的方法，在不作出实质性牺牲的前提下较好地克服了上述矛盾.

前馈网络的另一弱点是“熵漏”. 例如，若网络函数 $f(x_1,\cdots,x_n)$ 能被某个线性布尔函数很好地逼近，那么相应的密码就可用 QBR 方法攻破. 正是用这种方法，曾肯成教授成功地破译了有名的 Geffe 序列[5]. 那么应该怎样设计 $f(x_1,\cdots,x_n)$ 才能使线性逼近的 QBR 方法失灵呢？这是本文第三节所要回答的问题.

二、广义相关免疫度的概念

相关免疫度是密码抗击“相关攻击法”的能力之度量指标. 而“相关攻击法”并非万能的. 如果从某些输入中所能获得的有关输出的信息量 ε 足够小，那么“相关攻击法”就会失效. 也许是为了分析简单起见 Siegenthaler 将“ε 足够小”理解为“$\varepsilon = 0$”. 于是就出现了引言中介绍的矛盾，即线性复杂度成了相关免疫度的“牺牲品”. 下面分析将发现只要正确理解“ε 足够小”就能在不作出实质“牺牲”的前提下，较好地克服上述矛盾.

1989 年 11 月 8 日收到，1990 年 3 月 22 日修改定稿.
* 国家教委高校科研基金及国家青年自然科学基金资助课题.

定义 1　前馈网络函数(布尔函数)称为 m 阶 ε-相关免疫，当且仅当对任意 $x_{i_1},\cdots,x_{i_m}$ 和 $a_1,\cdots,a_m$ ($a_i=0$ 或 1) 恒有不等式：

$$|P(f(x_1,\cdots,x_n)=1)-P(f(x_1,\cdots,x_n)=1|x_{i_1}=a_1,\cdots,x_{i_m}=a_m)|\leqslant\varepsilon$$

其中 $P(\cdot)$ 和 $P(\cdot|\cdot)$ 分别表示概率和条件概率。不难看出当 $\varepsilon=0$ 时定义 1 中的广义相关免疫度就退化为 Siegenthaler 的狭义相关免疫度。

引理 1　布尔函数 $f(x_1,\cdots,x_n)$ 是 m 阶 ε-相关免疫，当且仅当恒成立：

$$\frac{1}{2^n}|W(f)-2^mW(f|x_{i_1}=a_1,\cdots,x_{i_m}=a_m)|\leqslant\varepsilon$$

其中 $W(f)$ 表示 n 元布尔函数 $f(\cdot)$ 的重量。x_{i_r} 和 a_j 的含义同定义 1。$W(f|x_{i_1}=a_1,\cdots,x_{i_m}=a_m)$ 表示在 $f(x_1,\cdots,x_n)$ 中固定 $x_{i_1}=a_1,\cdots,x_{i_m}=a_m$ 以后得到的 $(n-m)$ 元布尔函数的重量。

推论　如果 $f(x_1,\cdots,x_n)$ 是 m 阶 ε-相关免疫的，那么它也一定是 $(m-1)$ 阶 ε-相关免疫的。反之不一定成立。

定理 1　设 $f(x_1,\cdots,x_n)$ 是 m 阶 $(1\leqslant m\leqslant n-1)$ 狭义相关免疫的。令 $g(x_1,\cdots,x_n)=f(x_1,\cdots,x_n)+x_1x_2\cdots x_n$，那么 $g(x_1,\cdots,x_n)$ 是 m 阶 $(2^m+1)/2^n$-相关免疫的。

证明　由狭义相关免疫的定义知[6]，对任意 $x_{i_1},\cdots,x_{i_m}$ 和 $a_1,\cdots,a_m$ 都成立：

$$\frac{1}{2^n}|W(f)-2^mW(f|x_{i_1}=a_1,\cdots,x_{i_m}=a_m)|=0$$

现在 $W(g)=1+W(f)-2W(x_1\cdots x_nf(\cdot))=1+W(f)-2\delta_1$。(其中当 $f(\cdot)$ 中含偶数个单项式时 $\delta_1=0$，否则 $\delta_1=1$)。

当 $a_1=\cdots=a_m=1$ 时，$W(g|x_{i_1}=a_1,\cdots,x_{i_m}=a_m)=1+W(f|x_{i_1}=1,\cdots,x_{i_m}=1)-2\delta_2$。(其中当 $n-m$ 元布尔函数 $f(x_1,\cdots,x_n|x_{i_1}=\cdots=x_{i_m}=1)$ 中含有偶数个单项式时 $\delta_2=0$，否则 $\delta_2=1$)。

当 $a_1,\cdots,a_m$ 不全为 1 时，即 $a_1a_2\cdots a_m=0$ 时，

$$W(g|x_{i_1}=a_1,\cdots,x_{i_m}=a_m)=W(f|x_{i_1}=a_1,\cdots,x_{i_m}=a_m)$$

因此若令 $\delta=a_1a_2\cdots a_m$，那么

$$\frac{1}{2^n}|W(g)-2^mW(g|x_{i_1}=a_1,\cdots,x_{i_m}=a_m)|$$

$$=\frac{1}{2^n}|W(f)+1-2\delta_1-2^m[W(f|x_{i_1}=a_1,\cdots,x_{i_m}=a_m)+\delta(1-2\delta_2)]|$$

$$=\frac{1}{2^n}|1-2\delta_1+2^m\delta(1-2\delta_2)|\leqslant\frac{2^m+1}{2^n}$$　　证毕

注　在实际中有理由将 2^{-32} 看成 0，因此由定理 1 知，当 $n-m\geqslant 32$ 时 $g(x_1,\cdots,x_n)$ 是 ε 很小的 m 阶相关免疫，同时其线性复杂度又达到最大值。可见在定义 1 中广义相关免疫的意义下并在一定范围内线性复杂度已经不再是相关免疫的牺牲品了。当然此处的 $g(x_1,\cdots,x_n)$ 也不是理想的网络函数。

引理 2[7]　设 $f_1(x_1,\cdots,x_n)=\sum_{i=1}^{n}a_ix_1\cdots x_{i-1}x_{i+1}\cdots x_n+bx_1x_2\cdots x_n$，又记 $S=$

$\sum_{i=1}^{n} a_i \geqslant 1$，那么

$$W(f_1) = 2\left[\frac{S+1-b}{2}\right] + b \leqslant 2\left[\frac{n+1-b}{2}\right] + b$$

定理 2 设 $f(x_1,\cdots,x_n)$ 具有m阶狭义相关免疫，$f_1(x_1,\cdots,x_n)$ 是重量很小的布尔函数。若令 $g(x_1,\cdots,x_n) = f(x_1,\cdots,x_n) + f_1(x_1,\cdots,x_n)$，那么 $g(x_1,\cdots,x_n)$ 就是m阶 $[(1/2^n)(3+2^{m+1})W(f_1)]$-相关免疫的。

定理 3 若 $W(f(x_1,\cdots,x_n) + f(1+x_1,\cdots,1+x_n)) \leqslant \varepsilon$，那么 $f(x_1,\cdots,x_n)$ 就是 1 阶 $\varepsilon/2^n$-相关免疫的。

证明

$$\frac{1}{2^n}|W(f) - 2W(f|x_i = a_i)|$$

$$= \frac{1}{2^n}|W(f|x_i = a_i) + W(f|x_i = a_i + 1) - 2W(f|x_i = a_i)|$$

$$= \frac{1}{2^n}|W(f|x_i = 1 + a_i) - W(f|x_i = a_i)|$$

$$= \frac{1}{2^n}\sum_{x}[f(x_1,\cdots,x_{i-1},0,x_{i+1},\cdots,x_n) + f(1+x_1,\cdots,1 + x_{i-1},1,1+x_{i+1},\cdots,1+x_n)]$$

$$\leqslant \frac{1}{2^n}W(f(x_1,\cdots,x_n) + f(1+x_1,\cdots,1+x_n)) \leqslant \frac{\varepsilon}{2^n}$$ 证毕

定理 4 设 $f_1(x_1,\cdots,x_n)$ 是m阶 ε_1-相关免疫的，$f_2(x_1,\cdots,x_n)$ 是m阶 ε_2-相关免疫的，并且还有 $W(f_1) = W(f_2)$。若令 $f(x_1,\cdots,x_n,x_{n+1}) = x_{n+1}f_1(x_1,\cdots,x_n) + (1+x_{n+1})f_2(x_1,\cdots,x_n)$，那么 $f(x_1,\cdots,x_n,x_{n+1})$ 就是m阶 ε-相关免疫的。其中 $\varepsilon = \max(\varepsilon_1,\varepsilon_2)$。

证明 当 $i_m \neq n+1$ 时（此处已设 $i_1 < \cdots < i_m$），$W(f|x_{i_1} = a_1,\cdots,x_{i_m} = a_m) = W(f_1|x_{i_1} = a_1,\cdots,x_{i_m} = a_m) + W(f_2|x_{i_1} = a_1,\cdots,x_{i_m} = a_m)$ 于是

$$\frac{1}{2^{n+1}}|W(f) - 2^m W(f|x_{i_1} = a_1,\cdots,x_{i_m} = a_m)|$$

$$= \frac{1}{2^{n+1}}|W(f_1) + W(f_2) - W(f_1|x_{i_1} = a_1,\cdots,x_{i_m} = a_m) - W(f_2|x_{i_1} = a_1,\cdots,x_{i_m} = a_m)|$$

$$\leqslant \frac{1}{2}(\varepsilon_1 + \varepsilon_2) \leqslant \varepsilon \triangleq \max(\varepsilon_1,\varepsilon_2)$$

当 $i_m = n+1$ 时，

$W(f|x_{i_1} = a_1,\cdots,x_{i_{m-1}} = a_{m-1},x_{i_m} = 0) = W(f_2|x_{i_1} = a_1,\cdots,x_{i_{m-1}} = a_{m-1})$

$W(f|x_{i_1} = a_1,\cdots,x_{i_{m-1}} = a_{m-1},x_{i_m} = 1) = W(f_1|x_{i_1} = a_1,\cdots,x_{i_{m-1}} = a_{m-1})$

由 $W(f_1) = W(f_2)$ 和引理 1 的推论知：

$$\frac{1}{2^{n+1}}|W(f) - 2^m W(f|x_{i_1} = a_1,\cdots,x_{i_{m-1}} = a_{m-1},x_{i_m} = 0)|$$

$$= \frac{1}{2^{n+1}}|2W(f_2) - 2^m W(f_2|x_{i_1}=a_1,\cdots,x_{i_{m-1}}=a_{m-1})|$$

$$= \frac{1}{2^n}|W(f_2) - 2^{m-1}W(f_2|x_{i_1}=a_1,\cdots,x_{i_{m-1}}=a_{m-1}|$$

$$\leqslant \varepsilon_2 \leqslant \max(\varepsilon_1,\varepsilon_2)$$

同理可得

$$\frac{1}{2^{n+1}}|W(f) - 2^m W(f|x_{i_1}=a_1,\cdots,x_{i_{m-1}}=a_{m-1},x_{i_m}=a_m)| \leqslant \max(\varepsilon_1,\varepsilon_2)$$ 证毕

定理 5　设 $f_1(x_1,\cdots,x_n),\cdots,f_{2^k}(x_1,\cdots,x_n)$ 分别是 m 阶 ε_i-相关免疫的（其中 $1\leqslant i\leqslant 2^k$），并且 $W(f_1)=W(f_2)=\cdots=W(f_{2^k})$。记 $\varepsilon=\max\limits_{1\leqslant i\leqslant 2^k}\{\varepsilon_i\}$。令 $g(x_1,\cdots,x_n,y_1,\cdots,y_k)=\sum\limits_{\underline{a}} y_1^{(a_1)}\cdots y_k^{(a_k)}f_{\underline{a}}(x_1,\cdots,x_n)$，那么 $g(x_1,\cdots,x_n,y_1,\cdots,y_k)$ 是 m 阶 ε-相关免疫的。其中 $a_i=0$ 或 1，$\underline{a}=(a_1,\cdots,a_k)$，$y^{(0)}=1+y$，$y^{(1)}=y$。

当 $k=1$ 时定理 5 就退化成定理 4。

定理 6　设 $f(x_1,\cdots,x_n)$ 是 m 阶 ε-相关免疫的。在任意固定 $x_{r+1}=b_{1+r},\cdots,x_n=b_n$ 后，若令 $g(x_1,\cdots,x_r)=f(x_1,\cdots,x_r,b_{r+1},\cdots,b_n)$，那么 $g(x_1,\cdots,x_r)$ 是 $(m-n+r)$ 阶 ε-相关免疫的。

定理 7　设 $f_1(x_1,\cdots,x_{n_1})$ 是 m_1 阶 ε_1-相关免疫的，$f_2(y_1,\cdots,y_{n_2})$ 是 m_2 阶 ε_2-相关免疫的，$m_1<m_2$。若令 $f(x_1,\cdots,x_{n_1},y_1,\cdots,y_{n_2})=f_1(x_1,\cdots,x_{n_1})+f_2(y_1,\cdots,y_{n_2})$，那么，(1)如果 $W(f_1)=2^{n_1-1}$，$W(f_2)=2^{n_2-1}$ 则 $f(x_1,\cdots,x_{n_1},y_1,\cdots,y_{n_2})$ 就是 m_1+m_2+1 阶 (2ε)-相关免疫的。此处 $\varepsilon=\max(\varepsilon_1,\varepsilon_2)$；(2) 如果 $W(f_1)\neq 2^{n_1-1}$，$W(f_2)=2^{n_2-1}$，则 $f(\cdot)$ 是 m_2 阶 $(2\varepsilon_2)$-相关免疫的；(3) 如果 $W(f_2)\neq 2^{n_2-1}$，则 $f(\cdot)$ 就是 m_1 阶 $(2\varepsilon_1)$-相关免疫的。

证明　首先注意 $W(f)=2^{n_2}W(f_1)+2^{n_1}W(f_2)-2W(f_1)W(f_2)$。现在来证明 (1)。由于 $W(f_1)=2^{n_1-1}$，$W(f_2)=2^{n_2-1}$，所以 $W(f)=2^{n_1+n_2-1}$。任意固定 $x_{i_1}=a_1,\cdots,x_{i_r}=a_r,y_{j_1}=b_1,\cdots,y_{j_{m_1+m_2+1-r}}=b_{m_1+m_2+1-r}$ 之后有两种情况：

情况 1　$r\leqslant m_1$，此时必有

$$\frac{1}{2^{n_1}}|W(f_1) - 2^{m_1}W(f_1|x_{i_1}=a_1,\cdots,x_{i_r}=a_r)| \leqslant \varepsilon_1$$

于是

$$\frac{1}{2^{n_1+n_2}}|W(f) - 2^{m_1+m_2+1}W(f|x_{i_1}=a_1,\cdots,x_{i_r}=a_r,$$

$$y_{j_1}=b_1,\cdots,y_{j_{m_1+m_2+1-r}}=b_{m_1+m_2+1-r})|$$

$$= \frac{1}{2^{n_1+n_2}}|2^{n_1+n_2-1} - 2^{m_1+m_2+1}[2^{n_2-(m_1+m_2+1-r)}W(f_1|x_{i_1}=a_1,\cdots,x_{i_r}=a_r)$$

$$+ 2^{n_1-r}W(f_2|y_{j_1}=b_1,\cdots,y_{j_{m_1+m_2+1-r}}=b_{m_1+m_2+1-r})$$

$$- 2W(f_1|x_{i_1}=a_1,\cdots,x_{i_r}=a_r)W(f_2|y_{j_1}=b_1,\cdots,$$

$$y_{j_{m_1+m_2+1-r}}=b_{m_1+m_2+1-r})]|$$

$$\leqslant \frac{1}{2^{n_1}}|2^{n_1-1} - 2^r W(f_1|x_{i_1}=a_1,\cdots,x_{i_r}=a_r)|$$

$$+\frac{1}{2^{n_1}}|2^{n_1-1-r}-W(f_1|x_{i_1}=a_1,\cdots,x_{i_r}=a_r)|$$

$$\leqslant \varepsilon_1+\frac{1}{2^r}\varepsilon_1\leqslant 2\varepsilon_1\leqslant 2\max(\varepsilon_1,\varepsilon_2)$$

情况 2　$r\geqslant m_1+1$，于是 $m_1+m_2+1-r\leqslant m_2$。仿上步骤可证此时有

$$\frac{1}{2^{n_1+n_2}}|W(f)-2^{m_1+m_2+1}W(f|x_{i_1}=a_1,\cdots,x_{i_r}=a_r,$$

$$y_{i_1}=b_1,\cdots,y_{i_{m_1+m_2+1-r}}=b_{m_1+m_2+1-r})|\leqslant 2\varepsilon_2\leqslant 2\max(\varepsilon_1,\varepsilon_2)$$

综合情况 1，2 就完成了(1)的证明。(2)和(3)可用同法证明。略去。　证毕

定理 8　如果 $f(x_1,\cdots,x_n)$ 是 m 阶 ε-相关免疫的，那么对任意线性布尔函数 $g(x_1,\cdots,x_n)=\sum_{i=1}^{n}c_ix_i$，只要 $\sum_{i=1}^{n}c_i\leqslant m$ 就恒有：

$$\frac{1}{2^n}|W(f(x_1,\cdots,x_n)+g(x_1,\cdots,x_n))-2^{n-1}|\leqslant\varepsilon$$

证明　不妨设 $c_{i_1}=c_{i_2}=\cdots=c_{i_r}=1$，$(r\leqslant m)$，并且其它的 c_i 全为 0。记 $A=\left\{(x_1,\cdots,x_n):\sum_{i=1}^{n}c_ix_i=1\right\}$ 显然 $|A|=2^{r-1}$（此处 $|A|$ 表示集合的容量）。于是

$$\frac{1}{2^n}|W(f(x_1,\cdots,x_n)+g(x_1,\cdots,x_n))-2^{n-1}|$$

$$=\frac{1}{2^n}|W(f)+2^{n-1}-2W\left[\left(\sum_{i=1}^{n}c_ix_i\right)f(x_1,\cdots,x_n)\right]-2^{n-1}|$$

$$=\frac{1}{2^n}\left|W(f)-2\sum_{a\in A}W(f|x_{i_1}=a_1,\cdots,x_{i_r}=a_r)\right|$$

$$=\frac{1}{2^n}\left|2^{-r+1}\sum_{a\in A}[W(f)-2^rW(f|x_{i_1}=a_1,\cdots,x_{i_r}=a_r)]\right|$$

$$\leqslant 2^{-r+1}\sum_{a\in A}\frac{1}{2^n}|W(f)-2^rW(f|x_{i_1}=a_1,\cdots,x_{i_r}=a_r)|$$

$$\leqslant 2^{-r+1}\sum_{a\in A}\varepsilon=\varepsilon$$　证毕

三、线性逼近熵漏研究

上节讨论了一种特殊的熵漏现象——相关免疫性。本节再讨论另一种与之密切相关的熵漏现象——线性逼近熵漏。正如引言中所述，当网络函数能被某个线性布尔函数很好地逼近时，QBR 攻击法就对相应的密码构成严重威胁。因此当对任意线性布尔函数 $b+\sum_{i=1}^{n}c_ix_i$ 都成立 $W(f(x_1,\cdots,x_n)+b+\sum_{i=1}^{n}c_ix_i)\approx 2^{n-1}$ 时，相应的 $f(\cdot)$ 就具有较强的抗 QBR 攻击能力。

由上节定理 8 可知，如果 $f(x_1,\cdots,x_n)$ 是 m 阶 ε-相关免疫的，那么它就不可能被项数小于 $m+1$ 的线性布尔函数很好地逼近。可见相关免疫与线性逼近熵漏之间既有密切

的联系又不能彼此代替。

定义 2　$f(x_1,\cdots,x_n)$ 是 n 元布尔函数，如果对任意线性布尔函数 $b+\sum_{i=1}^{n}c_ix_i$ 恒成立

$$\frac{1}{2^n}\left|W(f(x_1,\cdots,x_n)+b+\sum_{i=1}^{a}c_ix_i)-2^{n-1}\right|\leqslant\delta$$

那么就称 $f(x_1,\cdots,x_n)$ 具有 δ-线性熵漏。

在定义 2 中，如果 δ 越小那么 $f(x_1,\cdots,x_n)$ 就越不能被很好地线性逼近，从而它抗击线性逼近 QBR 攻击法的能力就越强。

定理 9　Bent 函数[8] $f(x_1,\cdots,x_n)$ 的线性熵漏值 δ 很小。精确地说任意 n 元 Bent 函数都具有 $2^{-(\frac{n}{2}+1)}$-线性熵漏。

注意到，当 $n\to\infty$ 时，$2^{-(\frac{n}{2}+1)}\to 0$。所以定理 9 提供了一大类抗击 QBR 攻击能力较好的网络函数。将定理 9 与如下定理 10 结合起来，便可设计出更多的具有良好线性熵漏特性的前馈网络函数。

定理 10　如果 $f_1(x_1,\cdots,x_n)$ 具有 δ_1-线性熵漏，$f_2(x_1,\cdots,x_n)$ 是一个重量很小的布尔函数。不妨设 $\frac{1}{2^n}W(f_2)=\delta_2$ (δ_2 很小)。若令 $g(x_1,\cdots,x_n)=f_1(x_1,\cdots,x_n)+f_2(x_1,\cdots,x_n)$，那么 $g(x_1,\cdots,x_n)$ 具有 $(\delta_1+\delta_2)$-线性熵漏。

证明

$$\begin{aligned}
&\frac{1}{2^n}\left|W\left(g(x_1,\cdots,x_n)+b+\sum_{i=1}^{n}c_ix_i\right)-2^{n-1}\right|\\
&=\frac{1}{2^n}\left|W\left(f_2(x_1,\cdots,x_n)+f_1(x_1,\cdots,x_n)+b+\sum_{i=1}^{n}c_ix_i\right)-2^{n-1}\right|\\
&=\frac{1}{2^n}\left|B+W(f_1(x_1,\cdots,x_n)+b+\sum_{i=1}^{n}c_ix_i)-2^{n-1}\right|\\
&\leqslant\frac{1}{2^n}|B|+\frac{1}{2^n}\left|W\left(f_1(x_1,\cdots,x_n)+b+\sum_{i=1}^{n}c_ix_i\right)-2^{n-1}\right|
\end{aligned}$$

其中 $|B|$ 是一个与 $f_1(\cdot)$ 和 $b+\sum_{i=1}^{n}c_ix_i$ 都有关的整数(可正，可负)，并且 $|B|\leqslant W(f_2)$，于是

$$\frac{1}{2^n}\left|W\left(g(x_1,\cdots,x_n)+b+\sum_{i=1}^{n}c_ix_i\right)-2^{n-1}\right|\leqslant\delta_1+\delta_2$$　　证毕

上面的定理 10 告诉我们，网络函数可以同时具有良好的线性熵漏特性和极大的线性复杂度。他们之间不存在折衷。

在给出下一定理之前先简述有关布尔函数 $f(x_1,\cdots,x_n)$ 的 Walsh 变换的定义和性质。

$$\hat{F}(u)\triangleq\hat{F}(u_1,\cdots,u_n)=\frac{1}{2^n}\sum_{x}(-1)^{x\cdot u+f(x)}$$

称为 $f(x_1,\cdots,x_n)$ 的 Walsh 变换。它有如下常见性质:

(a) 逆变换: $(-1)^{f(\underline{x})}=\sum_{\underline{u}}(-1)^{\underline{u}\cdot\underline{x}}\hat{F}(\underline{u})$;

(b) 能量守恒: $\sum_{\underline{u}}[\hat{F}(\underline{u})]^2=1$。

定理 11 $f(x_1,\cdots,x_n)$ 具有 δ-线性熵漏的充要条件是 $|\hat{F}(\underline{u})|\leqslant 2\delta$ 恒成立。

证明 由于

$$\hat{F}(\underline{u})=\frac{1}{2^n}\sum_{\underline{v}}(-1)^{\underline{u}\cdot\underline{v}+f(\underline{v})}=\frac{1}{2^n}\left[2^n-2W\left(f(x_1,\cdots,x_n)+\sum_{i=1}^{n}u_ix_i\right)\right]$$

所以

$$W\left(f(x_1,\cdots,x_n)+\sum_{i=1}^{n}u_ix_i\right)=2^{n-1}(1-\hat{F}(\underline{u}))$$

$$W\left(f(x_1,\cdots,x_n)+\sum_{i=1}^{n}u_ix_i+1\right)=2^{n-1}(1+\hat{F}(\underline{u}))$$

$$\frac{1}{2^n}\left|W\left(f(x_1,\cdots,x_n)+b+\sum_{i=1}^{n}c_ix_i-2^{n-1}\right.\right|=\frac{1}{2^n}|2^{n-1}(1\pm\hat{F}(\underline{u}))-2^{n-1}|$$

$$=\frac{1}{2}|\hat{F}(\underline{u})|$$

再利用定义 2 就证明了。 证毕

推论 如果 $f(x_1,\cdots,x_n)$ 能使等式

$$\frac{1}{2^n}\left|W\left(f(x_1,\cdots,x_n)+b+\sum_{i=1}^{n}c_ix_i\right)-2^{n-1}\right|=\delta$$

恒成立,那么 $f(x_1,\cdots,x_n)$ 一定是 Bent 函数,并且 $\delta=2^{-(\frac{n}{2}+1)}$。

从上述推论可见,Bent 函数在具有良好线性逼近熵漏特性的网络函数中占有非常独特的地位。

证明 由定理 11 的证明过程知此时恒有 $|\hat{F}(\underline{u})|=2\delta$,再由能量守恒定理 $\sum_{\underline{u}}|\hat{F}(\underline{u})|^2=1$,就知 $4\delta^2\cdot 2^n=1$,$\delta=2^{-(\frac{n}{2}+1)}$。于是 $\hat{F}(\underline{u})=\pm 2^{-\frac{n}{2}}$,$2^n\hat{F}(\underline{u})=\pm 2^{\frac{n}{2}}$。这就是说 $f(x_1,\cdots,x_n)$ 的 Hadamard 系数恒为 $2^{\frac{n}{2}}$,由文献[8]第 426 页的定义知 $f(x_1,\cdots,x_n)$ 必定是 Bent 函数。 证毕

定理 12 如果 $f(x_1,\cdots,x_n)$ 具有 δ-线性熵漏,那么对任意 $\underline{y}=(y_1,\cdots,y_n)\neq(0,\cdots,0)$ 恒有

$$\frac{1}{4^n}|W[f(x_1,\cdots,x_n)+f(x_1+y_1,,\cdots,x_n+y_n)]-2^{n-1}|\leqslant\delta^2$$

证明 由 Walsh 逆变换可知:

$$\sum_{\underline{x}}(-1)^{f(\underline{x})+f(\underline{x}+\underline{y})}=\sum_{\underline{x}}(-1)^{f(\underline{x})}(-1)^{f(\underline{x}+\underline{y})}$$

$$=\sum_{\underline{x}}\left[\sum_{\underline{u}}(-1)^{\underline{u}\cdot\underline{x}}\hat{F}(\underline{u})\right]\left[\sum_{\underline{w}}(-1)^{(\underline{x}+\underline{y})\cdot\underline{w}}\hat{F}(\underline{w})\right]$$

$$= \sum_{\underline{u}} \sum_{\underline{w}} (-1)^{\underline{y}\cdot\underline{w}} \hat{F}(\underline{u})\hat{F}(\underline{w}) \left[\sum_{\underline{x}} (-1)^{\underline{x}\cdot(\underline{u}+\underline{w})}\right]$$

$$= 2^n \sum_{\underline{u}} (-1)^{\underline{y}\cdot\underline{u}} |\hat{F}(\underline{u})|^2$$

另一方面，$\sum_{\underline{x}} (-1)^{f(\underline{x})+f(\underline{x}+\underline{y})} = 2^n - 2W[f(x_1, \cdots, x_n) + f(x_1 + y_1, \cdots, x_n + y_n)]$，于是有

$$|2^{n-1} - W[f(x_1, \cdots, x_n) + f(x_1 + y_1, \cdots, x_n + y_n)]|$$

$$= \left|2^{n-1} \sum_{\underline{u}} (-1)^{\underline{y}\cdot\underline{u}} (\hat{F}(\underline{u}))^2\right|$$

$$= 2^{n-1} \left| \sum_{\underline{u}\cdot\underline{y}=0} (\hat{F}(\underline{u}))^2 - \sum_{\underline{u}\cdot\underline{y}=1} (\hat{F}(\underline{u}))^2 \right|$$

再由定理 11 的 $|\hat{F}(\underline{u})| \leqslant 2\delta$，立即知：

$$|2^{n-1} - W[f(x_1, \cdots, x_n) + f(x_1 + y_1, \cdots, x_n + y_n)]|$$

$$\leqslant 2^{n-1} \cdot 2^{n-1} \cdot 4\delta^2 = 4^n\delta^2$$　　证毕

定理 13　设 $f(x_1, \cdots, x_n)$ 具有 δ_1-线性熵漏，$g(y_1, \cdots, y_m)$ 具有 δ_2-线性熵漏，$\delta_1 \leqslant \delta_2$。若令 $h(x_1, \cdots, x_n, y_1, \cdots, y_m) = f(x_1, \cdots, x_n) + g(y_1, \cdots, y_m)$，那么 $h(x_1, \cdots, x_n, y_1, \cdots, y_m)$ 就具有 $2\delta_1(1 + \delta_2)$-线性熵漏。

证明　因为 $g(y_1, \cdots, y_m)$ 具有 δ_2-线性熵漏，所以

$$\frac{1}{2^m}\left|W\left[g(y_1, \cdots, y_m) + b + \sum_{i=1}^{m} a_i y_i\right] - 2^{m-1}\right| \leqslant \delta_2,$$

即

$$2^{m-1} - 2^m\delta_2 \leqslant W\left[g(y_1, \cdots, y_m) + b + \sum_{i=1}^{m} a_i y_i\right] \leqslant 2^{m-1} + 2^m\delta_2,$$

从而

$$\frac{1}{2^{m-1}} W\left[g(y_1, \cdots, y_m) + b + \sum_{i=1}^{m} a_i y_i\right] \leqslant 1 + 2\delta_2$$

另一方面

$$\frac{1}{2^{m+n}}\left|W\left[f(x_1, \cdots, x_n) + g(y_1, \cdots, y_m) + \sum_{i=1}^{n} c_i x_i + \sum_{i=1}^{m} a_i y_i + b\right] - 2^{m+n-1}\right|$$

$$= \frac{1}{2^{m+n}}\left|2^m W\left[f(x_1, \cdots, x_n) + \sum_{i=1}^{n} c_i x_i\right] + 2^n W\left[g(y_1, \cdots, y_m) + b + \sum_{i=1}^{m} a_i y_i\right]\right.$$

$$\left. - 2W\left[f(x_1, \cdots, x_n) + \sum_{i=1}^{n} c_i x_i\right] W\left[g(y_1, \cdots, y_m) + b + \sum_{i=1}^{m} a_i y_i\right] - 2^{m+n-1}\right|$$

$$\leqslant \frac{1}{2^n}\left|W\left[f(x_1, \cdots, x_n) + \sum_{i=1}^{n} a_i x_i\right] - 2^{n-1}\right|$$

$$+ \frac{1}{2^{m+n-1}} W\left[g(y_1, \cdots, y_m) + b + \sum_{i=1}^{m} a_i y_i\right]\left|2^{n-1} - W\left[f(x_1, \cdots, x_n)\right.\right.$$

$$+\sum_{i=1}^{n} c_i x_i\Big]\Big| \leqslant \delta_1 + \delta_1(1+2\delta_2) = 2\delta_1(1+\delta_2)$$ 证毕

定理 14 设布尔函数 $f(x_1,\cdots,x_n)$ 和 $f_2(x_1,\cdots,x_n)$ 分别具有 δ_1-线性熵漏和 δ_2-线性熵漏，那么 $f(x_1,\cdots,x_n,x_{n+1}) = x_{n+1}f_1(x_1,\cdots,x_n) + (1+x_{n+1})f_2(x_1,\cdots,x_n)$ 具有 $\frac{1}{2}(\delta_1+\delta_2)$-线性熵漏。

证明

$$\begin{aligned}
&\frac{1}{2^{n+1}}\left|W\left(f(x_1,\cdots,x_{n+1}) + \sum_{i=1}^{n} a_i x_i + b x_{n+1} + c\right) - 2^n\right| \\
&= \frac{1}{2^{n+1}}\left|W\left[f_2(x_1,\cdots,x_n) + \sum_{i=1}^{n} a_i x_i + c\right] + W\left[f_1(x_1,\cdots,x_n) + b\right.\right. \\
&\quad \left.\left. + c + \sum_{i=1}^{n} a_i x_i\right] - 2^n\right| \\
&\leqslant \frac{1}{2}\left\{\frac{1}{2^n}\left|W\left[f_2(x_1,\cdots,x_n) + c + \sum_{i=1}^{n} a_i x_i\right] - 2^{n-1}\right|\right. \\
&\quad \left. + \frac{1}{2^n}\left|W\left[f_1(x_1,\cdots,x_n) + b + c + \sum_{i=1}^{n} a_i x_i\right] - 2^{n-1}\right|\right\} \\
&\leqslant \frac{1}{2}(\delta_1+\delta_2)
\end{aligned}$$ 证毕

仿上节的定理 5，此定理还可推广为以下推论。

推论 设 $f_i(x_1,\cdots,x_n)$，$(1 \leqslant i \leqslant 2^k)$ 是 2^k 个布尔函数，它们分别具有 δ_i-线性熵漏。令

$$f(x_1,\cdots,x_n,y_1,\cdots,y_k) = \sum_{a} y_1^{(a_1)}\cdots y_k^{(a_k)} f_a(x_1,\cdots,x_n)$$

那么 $f(x_1,\cdots,x_n,y_1,\cdots,y_k)$ 具有 $\left(2^{-k}\sum_{i=1}^{2^k}\delta_i\right)$-线性熵漏。

当 $k=1$ 时，此推论退化为定理 14。

参 考 文 献

[1] T. Siegenthaler, IEEE Int. Symp. Inform. Theory, Saint Jovite, Canada, 26—29, Sept. (1983).

[2] T. Siegenthaler, *IEEE Trans. on IT* **IT-30**(1984), 776—780.

[3] T. Siegenthaler, *IEEE Trans. on C*, **C-34**(1985), 81—85.

[4] R. Rueppel, Analysis and Design of Stream Ciphers, Springer-Verlag, New York, (1986).

[5] 曾肯成，密码体制中的熵漏现象，中科院研究生院数据处理中心报告，1988年.

[6] Yang Yi Xian, *IEE Electronics Letters*, **23**(1987), 1335—1336.

[7] 杨义先，北京邮电学院学报，1988 年，第 3 期，第 1—10 页.

[8] F. Macwilliams, N. Sloane, The Theory of Error-Correcting Codes, North-Holland, New York, (1977).

ON ENTROPY IMMUNITY OF FEEDFORWARD NETWORKS

Yang Yixian Hu Zhengming

(Beijing University of Posts and Telecommunications, Beijing)

Abstract From practical point of view, the Siegenthaler's definition of correlation immunity is improved. Under the new definition there exists no trade-off between the generalized correlation immunity and linear complexity of the output key streams. The famous Bent functions are used for the study of entropy immunity in feedforward netforks. New results and new methods are also presented.

Key words Cryptography; Feedforward networks; Correlation immunity; Entropy immunity