文章编号:1001 - 2486(2004)03 - 0043 - 05

对 DES 密码的一种新的线性分析*

李　超[1,2,3],屈龙江[1],李　强[1]
(1. 国防科技大学理学院,湖南 长沙　410073;　2. 国防科技大学计算机学院,湖南 长沙　410073;
3. 东南大学移动通信国家重点实验室,江苏 南京　210018)

摘　要:首先推广了变换的线性偏差的概念,然后利用它把密码体制线性偏差的数学描述也进行了推广,给出了 DES 密码的线性偏差与轮函数 F 的线性偏差的关系,确定了 DES 密码 16 轮以内各轮的线性偏差上界。

关键词:DES;线性分析;线性偏差
中图分类号:TN918.1　　文献标识码:A

A New Linear Cryptanalysis of DES Cipher

LI Chao[1,2,3], QU Long-jiang[1], LI Qiang[1]
(1. College of Science, National Univ. of Defense Technology, Changsha 410073, China;　2. College of Computer, National Univ. of Defense Technology, Changsha 410073, China;　3. State Key Laboratory of Mobile of Southeast Univ., Nanjing 210018, China)

Abstract: Firstly, generalize the definition of the linear bias of transformation, and then generalize the mathematical description of the linear bias of cipher, and present the relation between the linear bias of cipher and the linear bias of round function F. The upper bound of linear bias of each round within 16 rounds in DES cipher is finally given.

Key words: DES; linear cryptanalysis; linear bias

文献[1]中提出了变换的线性偏差和密码线性偏差的概念,并给出了密码线性偏差的上界。但其中的方法只适用于轮函数是双射的情况,对于轮函数不是双射的情况,例如 DES,它就不适用了。在本文中,考虑把文献[1]中的方法推广,从而能对 DES 类密码进行这种分析。

用(X_0^i, X_1^i)表示 DES 第 i 轮$(0 \leqslant i < r)$的状态,则密码的一轮变换公式为

$$X_0^{i+1} = X_1^i, \quad X_1^{i+1} = X_0^i \oplus F(E(X_1^i) \oplus k_i)$$

其中,$i = 0, 1, \cdots, r-1$,r 为密码变换的总轮数。

首先推广文献[1]中定义的变换的线性偏差的概念。

定义 1　设 T 是 s 比特输入 t 比特输出的非线性变换,即 $T: Z_2^s \to Z_2^t$。对任意的 $w \in Z_2^s$, $v \in Z_2^t$,定义变换 T 的线性偏差为

$$LP^T(v, w) = 2^{-s} \sum_{x \in Z_2^s} (-1)^{[w \cdot x \oplus v \cdot T(x)]}$$

定义变换 T 的最大线性偏差为

$$LP_{\max}^T = \max_{w, v \neq 0} LP^T(v, w)$$

其中,"·"表示为两个向量的点积,称 w 为输入线性组合系数,v 为输出线性组合系数。

定义 2　设 T 是 s 比特输入 t 比特输出$(s \geqslant t)$的非线性变换,即 $T: Z_2^s \to Z_2^t$,若对 $\forall\, b \in Z_2^t$,都有 2^{s-t} 个 $a \in Z_2^s$,使得 $T(a) = b$,则称变换 T 是平衡的。

当 $w = 0$ 且 $v = 0$ 时,显然有 $LP^T(0,0) = 1$;而当 $w \neq 0$ 而 $v = 0$ 时,显然有 $LP^T(0, w) = 0$;而当 $w = 0$

* 收稿日期:2003 - 12 - 12
基金项目:东南大学移动通信国家重点实验室开放基金资助项目(A0307);国防科技大学基础研究基金资助项目(JC02 - 02 - 007)
作者简介:李超(1966—),男,教授,博士。

而 $v\neq 0$ 时，若还假设 T 为一平衡函数，有

$$LP^T(v,0) = 2^{-s}\sum_{x\in Z_2^s}(-1)^{v\cdot T(x)} = 2^{-s}\sum_{y\in Z_2^t}(-1)^{v\cdot y}\cdot 2^{s-t} = 2^{-t}\sum_{y\in Z_2^t}(-1)^{v\cdot y} = 0$$

从而有下述定理：

定理 1 设变换 T 为一平衡函数，则有：

(1) 如果 $w=0, v=0$，则 $LP^T(v,w)=1$；

(2) 如果 w 和 v 仅有一个为零，则 $LP^T(v,w)=0$。

上述两种情况下的线性偏差只可能是 0 或 1，称其为平凡的。

有时也直接用 $LP(w\cdot x\oplus v\cdot T(x))$ 表示变换 T 的输入输出线性偏差。若分组密码的明文 X、密钥 K 和对应的密文 Y 三者的线性组合系数分别为 W、V、U 时，其线性偏差定义为 $LP(W\cdot X\oplus V\cdot K\oplus U\cdot Y)$。在以下的表述中，线性偏差的大小总是指其绝对值的大小。

定义 3 对某个变换 T，如果它的输入输出线性组合系数均不为零，则称变换 T 是活动的。

1 密码线性偏差的数学描述

线性密码分析的基本原理是寻找明文、密文和密钥间的有效线性逼近式，当该逼近式的线性偏差足够大时，就可以由一定量的明密对推测部分密钥信息。线性分析的关键是确定有效线性逼近式的线性偏差和线性组合系数。理论上讲，线性分析应当利用明文、密文和原始密钥间的关系，但实际上寻找明文、密文和原始密钥间的有效线性逼近式是困难的，通常的做法是寻找明文、密文和子密钥之间的有效线性逼近式，并假设子密钥是独立的。

本文通过理论推导，给出了密码线性偏差和轮函数 F 的线性偏差的数学关系。在推导中，假定所有的子密钥变量是相互独立、均匀分布的。

设输入明文 X_0^0, X_1^0 均为 t 比特随机变量，子密钥 $k_0, k_1, \cdots, k_{r-1}$ 均为 s 比特随机变量(对 DES 而言，$s=48, t=32$)，且它们是相互独立均匀分布的。当输入 X_0^0, X_1^0、子密钥 $k_0, k_1, \cdots, k_{r-1}$ 和 r 轮迭代后相应的输出 X_0^r, X_1^r 的线性组合系数分别为 $w_0, w_1, v_0, \cdots, v_{r-1}, u_0, u_1$ ($w_0, w_1, u_0, u_1\in Z_2^t$；$v_0, \cdots, v_{r-1}\in Z_2^s$)时，定义密码的线性偏差为

$$LP(w_0X_0^0\oplus w_1X_1^0\oplus v_0k_0\oplus\cdots\oplus v_{r-1}k_{r-1}\oplus u_0X_0^r\oplus u_1X_1^r)$$

对于 DES 而言，它的轮函数 $F: Z_2^{48}\to Z_2^{32}$ 不是双射。在 X_1^i 进入轮函数之前，需经过一个线性扩展函数 E，把它从 32 比特扩展为 48 比特，然后和一个 48 比特的子密钥 k_i 相加，最后 $E(X_1^i)\oplus k_i$ 经过轮函数 F 作用又变回 32 比特。设 $a=(a_0,a_1,\cdots,a_{s-1})\in Z_2^s, b=(b_0,b_1,\cdots,b_{t-1})\in Z_2^t$，考虑 $a\cdot E(b)$，这里 $s=48, t=32$，E 为 DES 的扩展函数。若把 $a\cdot E(b)$ 写成 s 项形如 $a_ib_j(0\leqslant i\leqslant s-1, 0\leqslant j\leqslant t-1)$ 的乘积的和的形式，然后按 $b_j(0\leqslant j\leqslant t-1)$ 合并同类项，则 b 的系数向量 c 是 t 比特的，且其每一个分量都是 a 的某些分量的线性组合，由此可以定义一个压缩函数 $C: Z_2^s\to Z_2^t$，使得对于原来的扩展函数 E，有 $a\cdot E(b)=C(a)\cdot b$。从而有：

引理 1 若 E 为 DES 的线性扩展函数，$E: E_2^t\to Z_2^t (t\leqslant s)$，则存在一线性压缩函数 $C: Z_2^s\to Z_2^t$，使得对 $\forall a\in Z_2^s, \forall b\in Z_2^t$，都有 $a\cdot E(b)=C(a)\cdot b$。

现在可以给出线性偏差的一轮推导关系：

引理 2
$$LP(w_0X_0^0\oplus w_1X_1^0\oplus v_0k_0\oplus\cdots\oplus v_{k-1}k_{r-1}\oplus u_0X_0^r\oplus u_1X_1^r)$$
$$= LP^F(u_1, v_{r-1})LP(w_0X_0^0\oplus w_1X_1^0\oplus v_0k_0\oplus\cdots\oplus v_{r-2}k_{r-2}\oplus u_1X_0^{r-1}\oplus(u_0\oplus C(v_{r-1}))X_1^{r-1})$$

证明
$$LP(w_0X_0^0\oplus w_1X_1^0\oplus v_0k_0\oplus\cdots\oplus v_{r-1}k_{r-1}\oplus u_0X_0^r\oplus u_1X_1^r)$$
$$= \alpha\sum_{X_0^0, X_1^0\in Z_2^t; k_0,\cdots,k_{r-1}\in Z_2^s}(-1)^{(w_0X_0^0\oplus w_1X_1^0\oplus v_0k_0\oplus\cdots\oplus v_{r-1}k_{r-1}\oplus u_0X_0^r\oplus u_1X_1^r)} \tag{1}$$

将密码的非线性迭代关系代入(1)式，则有

$$(1)\text{式} = \alpha \sum_{X_0^0, X_1^0 \in Z_2^t; k_0, \cdots, k_{r-1} \in Z_2^t} (-1)^{(w_0 X_0^0 \oplus w_1 X_1^0 \oplus v_0 k_0 \oplus \cdots \oplus v_{r-1} k_{r-1} \oplus u_0 X_1^{r-1} \oplus u_1 (X_0^{r-1} \oplus F(E(X_1^{r-1}) \oplus k_{r-1}))}$$

$$= \alpha \sum_{X_0^0, X_1^0 \in Z_2^t; k_0, \cdots, k_{r-1} \in Z_2^t} [(-1)^{(w_0 X_0^0 \oplus w_1 X_1^0 \oplus v_0 k_0 \oplus \cdots \oplus v_{r-2} k_{r-2} \oplus u_0 X_1^{r-1} \oplus u_1 X_0^{r-1})} \cdot (-1)^{(v_{r-1} k_{r-1} \oplus u_1 F(E(X_1^{r-1}) \oplus k_{r-1}))}]$$

$$= \alpha \sum_{X_0^0, X_1^0 \in Z_2^t; k_0, \cdots, k_{r-2} \in Z_2^t} [(-1)^{(w_0 X_0^0 \oplus w_1 X_1^0 \oplus v_0 k_0 \oplus \cdots \oplus v_{r-2} k_{r-2} \oplus u_0 X_1^{r-1} \oplus u_1 X_0^{r-1} \oplus v_{r-1} E(X_1^{r-1}))}] \cdot$$

$$\sum_{k_{r-1} \in Z_2^t} (-1)^{(v_{r-1}(E(X_1^{r-1}) \oplus k_{r-1}) \oplus u_1 F(E(X_1^{r-1}) \oplus k_{r-1}))}$$

当 $X_0^0, X_1^0, k_0, \cdots, k_{r-2}$ 确定时,$E(X_1^{r-1})$ 是与 k_{r-1} 无关的定值,故可将 $E(X_1^{r-1}) \oplus k_{r-1}$ 视为一个变量,而又由引理 1,知有 $v_{r-1} \cdot E(X_1^{r-1}) = C(v_{r-1}) \cdot X_1^{r-1}$,从而有

$$(1)\text{式} = LP^F(u_1, v_{r-1})\alpha' \sum_{X_0^0, X_1^0 \in Z_2^t, k_0, \cdots, k_{r-2} \in Z_2^t} [(-1)^{(w_0 X_0^0 \oplus w_1 X_1^0 \oplus v_0 k_0 \oplus \cdots \oplus v_{r-2} k_{r-2} \oplus u_0 X_1^{r-1} \oplus u_1 X_0^{r-1} \oplus u_1 X_0^{r-1} \oplus C(v_{r-1}) X_1^{r-1})}]$$

$$= LP^F(u_1, v_{r-1}) LP(w_0 X_0^0 \oplus w_1 X_1^0 \oplus v_0 k_0 \oplus \cdots \oplus v_{r-2} k_{r-2} \oplus u_1 X_0^{r-1} \oplus (u_0 \oplus C(v_{r-1})) X_1^{r-1})$$

其中,$\alpha = 2^{-(2t+n)}$,$\alpha' = 2^{-[2t+(r-1)s]}$。 □

由引理 2 可以看到,经过一轮推导后,变量 k_{r-1}, X_0^r, X_1^r 在公式中消失了,所以反复使用上面的引理可以得到 4 轮迭代的线性偏差表达式:

$$LP^F(u_1, v_{r-1}) LP(w_0 X_0^0 \oplus w_1 X_1^0 \oplus v_0 k_0 \oplus \cdots \oplus v_{r-2} k_{r-2} \oplus u_1 X_0^{r-1} \oplus (u_0 \oplus C(v_{r-1})) X_1^{r-1})$$

$$= LP^F(u_1, v_{r-1}) LP^F(u_0 \oplus C(v_{r-1}), v_{r-2})$$

$$LP(w_0 X_0^0 \oplus w_1 X_1^0 \oplus v_0 k_0 \oplus \cdots \oplus v_{r-3} k_{r-3} \oplus (u_0 \oplus C(v_{r-1})) X_0^{r-2} \oplus (u_1 \oplus C(v_{r-2})) X_1^{r-2})$$

$$= LP^F(u_1, v_{r-1}) LP^F(u_0 \oplus C(v_{r-1}), v_{r-2}) LP^F(u_1 \oplus C(v_{r-2}), v_{r-3})$$

$$LP(w_0 X_0^0 \oplus w_1 X_1^0 \oplus v_0 k_0 \oplus \cdots \oplus v_{r-4} k_{r-4} \oplus (u_1 \oplus C(v_{r-2})) X_0^{r-3} \oplus (u_0 \oplus C(v_{r-1}) \oplus C(v_{r-3})) X_1^{r-3})$$

$$= LP^F(u_1, v_{r-1}) LP^F(u_0 \oplus C(v_{r-1}), v_{r-2}) LP^F(u_1 \oplus C(v_{r-2}), v_{r-3}) LP^F(u_0 \oplus C(v_{r-1}) \oplus C(v_{r-3}), v_{r-4})$$

$$LP(w_0 X_0^0 \oplus w_1 X_1^0 \oplus v_0 k_0 \oplus \cdots \oplus v_{r-5} k_{r-5} \oplus (u_0 \oplus C(v_{r-1}) \oplus C(v_{r-3})) X_0^{r-4} \oplus (u_1 \oplus C(v_{r-2}) \oplus C(v_{r-4})) X_1^{r-4})$$

定理 2　4 轮迭代的密码的线性偏差表达式为

$$LP(w_0 X_0^0 \oplus w_1 X_1^0 \oplus v_0 k_0 \oplus \cdots \oplus v_3 k_3 \oplus u_0 X_0^4 \oplus u_1 X_1^4)$$

$$= LP^F(u_1, v_3) LP^F(u_0 \oplus C(v_3), v_2) LP^F(u_1 \oplus C(v_2), v_1) LP^F(u_0 \oplus C(v_1) \oplus C(v_3), v_0)$$

$$LP((w_0 \oplus u_0 \oplus C(v_1) \oplus C(v_3)) X_0^0 \oplus (w_1 \oplus u_1 \oplus C(v_2) \oplus C(v_0)) X_1^0)$$

实际上,在上面表达式中最后一项是线性函数的线性偏差,由于变量 X_0^0, X_1^0 的随机性,为使整体偏差不为 0,其线性组合系数必须为 0,即应有

$$u_0 = w_0 \oplus C(v_1) \oplus C(v_3), \quad u_1 = w_1 \oplus C(v_2) \oplus C(v_0)$$

将以上关系代入定理 2 的表达式中,则它的最后一项为 1,定理 2 可以写为:

定理 3　4 轮迭代的密码的线性偏差表达式为:

$$LP(w_0 X_0^0 \oplus w_1 X_1^0 \oplus v_0 k_0 \oplus \cdots \oplus v_3 k_3 \oplus u_0 X_0^4 \oplus u_1 X_1^4)$$

$$= LP^F(w_0, v_0) LP^F(w_1 \oplus C(v_0), v_1) LP^F(w_0 \oplus C(v_1), v_2) LP^F(w_1 \oplus C(v_0) \oplus C(v_2), v_3)$$

且要求:

$$u_0 = w_0 \oplus C(v_1) \oplus C(v_3), \quad u_1 = w_1 \oplus C(v_2) \oplus C(v_0)$$

否则,密码的线性偏差为零。

实际上,定理 2 和定理 3 是等价的。可以看出,4 轮迭代的 DES 密码的线性偏差可以表示为 4 项轮函数 F 线性偏差的乘积,定理 2 中的表达式是输出线性组合系数和子密钥组合系数的函数,而定理 3 中的表达式是输入线性组合函数和子密钥组合系数的函数。由于后一种表达式更便于描述,所以使用后一种表达式。下面给出对任意 r 轮的密码线性偏差的数学表达式。

定理 4　r 轮迭代密码的线性偏差表达式为

$$LP(w_0 X_0^0 \oplus w_1 X_1^0 \oplus v_0 k_0 \oplus \cdots \oplus v_{r-1} k_{r-1} \oplus u_0 X_0^r \oplus u_1 X_1^r)$$

$$= \prod_{i=0}^{r-1} LP^F(w_{i \bmod 2} \oplus \sum_{j=0}^{[(i-1)/2]} C(v_{i-1-2j}), v_i)$$

其中，$i \bmod 2$ 表示 i 模 2 的余数，$[a]$表示不大于 a 的最小整数。

2 确定密码线性偏差上界

下面给出在得到线性偏差表达式的基础上确定线性偏差上界的算法。

算法的基本原理是：由于密码的线性偏差可以表示为轮函数 F 线性偏差乘积的形式，要使密码线性偏差取得最大值，需各乘积项中取值为 1 的项数尽可能地多，且不能出现取值为 0 的项。由定理 4 知，需输入输出同时取 0 的项数尽可能地多，且不能出现仅有一个为 0 的项，也就是输入输出线性组合系数均不为 0 的项数尽可能地少。获得这个项数，令每一项取最大值，就可以得出密码线性偏差的上界。这个问题可以通过求取线性方程组最小重量解的方法解决。目前关于求取线性方程组最小重量解尚无简便的方法，但可以通过计算机穷尽假设，利用对线性方程组进行初等变换的方式实现。方法是：

穷尽假设表达式中各线性偏差项中的活动项(输入输出系数均不为 0 的项)，用平凡项(输入输出系数均为 0 的项，是活动项以外的项)的方程通过初等变换去化简活动项方程，若可将任意活动项的输入或输出系数化简为 0，也就是说，由于某些项系数取 0 造成其它某些项系数必须取 0，则说明假设错误，否则假设正确。在穷尽假设中，采取活动项数从小到大的顺序，一旦出现正确假设，则该活动项数即为最小活动项数。

下面给出通过实际计算得出的密码线性偏差的上界 $LP_{\max}$ 与轮函数 F 的线性偏差上界 $LP^F_{\max}$ 的关系。以 8 轮迭代为例对所给算法的实现给予说明。由定理 4 可以得到 8 轮迭代密码的线性偏差表达式为

$$\begin{aligned}
&LP(w_0 X_0^0 \oplus w_1 X_1^0 \oplus v_0 k_0 \oplus \cdots \oplus v_7 k_7 \oplus u_0 X_0^8 \oplus u_1 X_1^8)\\
&= LP^F(w_0, v_0) LP^F(w_1 \oplus C(v_0), v_1) LP^F(w_0 \oplus C(v_1), v_2) LP^F(w_1 \oplus C(v_0) \oplus C(v_2), v_3)\\
&\quad LP^F(w_0 \oplus C(v_1) \oplus C(v_3), v_4) LP^F(w_1 \oplus C(v_0) \oplus C(v_2) \oplus C(v_4), v_5)\\
&\quad LP^F(w_0 \oplus C(v_1) \oplus C(v_3) \oplus C(v_5), v_6) LP^F(w_1 \oplus C(v_0) \oplus C(v_2) \oplus C(v_4) \oplus C(v_6), v_7) \qquad (2)
\end{aligned}$$

式(2)是 8 项轮函数 F 线性偏差的乘积，式中有 $w_0, w_1, v_0, \cdots, v_7$ 这 10 个变量，式中各项的输入输出系数都是这些变量的线性组合，写成关于上述变量的系数矩阵如图 1 所示。

上面矩阵每两行对应线性偏差表达式中一项，若式中某项为平凡项或活动项，则该项对应的系数矩阵中的两行对应的值记为 0 或 1(注意：这个值并不代表实际值，只是作为分类记号)。

在上面的表示中，有一个值得注意的问题：上面矩阵中，奇数行和偶数行对应的 $v_i(0 \leqslant i \leqslant 7)$的系数表示意义不同，偶数行的 v_i 就表示 v_i，但奇数行的 v_i 表示的却是 $C(v_i)$。而由于 $v_i = 0$ 能推出 $C(v_i) = 0$，但是 $C(v_i) = 0$ 却不能推出 $v_i = 0$(C 为压缩函数)，所以在对方程进行初等变换时，一定要注意这一点：对 v_i 的系数进行约化时，偶数行的 v_i 的系数为 0 能用来约化其它所有的行，但奇数行的 v_i 的系数为 0 却只能用来约化奇数行，而不能用来约化偶数行。

w_0	w_1	v_0	v_1	v_2	v_3	v_4	v_5	v_6	v_7
1	0	0	0	0	0	0	0	0	0
0	0	1	0	0	0	0	0	0	0
0	1	1	0	0	0	0	0	0	0
0	0	0	1	0	0	0	0	0	0
1	0	0	1	0	0	0	0	0	0
0	0	0	0	1	0	0	0	0	0
0	1	1	0	1	0	0	0	0	0
0	0	0	0	0	1	0	0	0	0
1	0	0	1	0	1	0	0	0	0
0	0	0	0	0	0	1	0	0	0
0	1	1	0	1	0	1	0	0	0
0	0	0	0	0	0	0	1	0	0
1	0	0	1	0	1	0	1	0	0
0	0	0	0	0	0	0	0	1	0
0	1	1	0	1	0	1	0	1	0
0	0	0	0	0	0	0	0	0	1

图 1 系数矩阵

Fig. 1 Coefficient matrix

按照前面所述方法穷尽，当活动项数为 1、2、3 时都出现矛盾。当活动项为 1、3、5、7 这 4 项时将方程分类放置，可得到增广矩阵，然后对其进行初等变换，如图 2 所示。

$$\begin{bmatrix}01100&00000&0\\00010&00000&0\\01101&00000&0\\00000&10000&0\\01101&01000&0\\00000&01010&0\\01101&01000&0\\00000&00100&0\\10000&00000&1\\00100&00000&1\\10010&00000&1\\00001&00000&1\\10010&10000&1\\00000&01000&1\\10010&10100&1\\00000&00010&1\end{bmatrix}\xrightarrow{\text{经初等变换变为}}\begin{bmatrix}01100&00000&0\\00010&00000&0\\00001&00000&0\\00000&10000&0\\00000&01000&0\\00000&00100&0\\00000&00010&0\\00000&00001&0\\10000&00000&1\\00100&00000&1\\10000&00000&1\\00001&00000&1\\10000&00000&1\\00000&01000&1\\10000&00000&1\\00000&00010&1\end{bmatrix}$$

图 2　初等变换

Fig.2　Transformation

可见,分类记号为 1 的行的系数没有出现全 0,说明假设没有出现矛盾。由化简后的矩阵可以得到组合系数的取值关系:

$$w_1 + C(v_0) = 0,\quad v_1 = v_3 = v_5 = v_7 = 0$$
$$C(v_2) = C(v_4) = C(v_6) = 0$$
$$w_0, v_0, v_2, v_4, v_6 \neq 0$$

这时实际上只有 5 个变量。将上述关系代入式(2),可以将线性偏差表示为 4 项的乘积:

$$LP(w_0 X_0^0 \oplus w_1 X_1^0 \oplus v_0 k_0 \oplus \cdots \oplus v_7 k_7 \oplus u_0 X_0^8 \oplus u_1 X_1^8)$$
$$= LP^F(w_0, v_0)\, LP^F(w_0, v_2)\, LP^F(w_0, v_4)\, LP^F(w_0, v_6)$$

由此可见,活动轮函数 F 最少项数为 4,可得:

$$LP_{\max} \leqslant (LP^F_{\max})^4$$

同理可求出任意 r 轮迭代最少活动轮函数 F 项数 $AN^F_{\min}$(如表 1 所示)。

表 1　1 ~ 16 轮的结果

Tab.1　Conclusion of 1 ~ 16 rounds

轮数	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$AN^F_{\min}$	1	1	1	2	2	3	3	4	4	5	5	6	6	7	7	8

3　结 论

本文推广了变换的线性偏差的概念,给出了 DES 密码的线性偏差与轮函数的线性偏差的关系,确定了 DES 密码 16 轮以内各轮的线性偏差上界,对于 DES 密码的线性分析有一定的意义。

参 考 文 献:

[1] 张如文．一类广义 Feistel 密码的线性分析[J]．中科院研究生院学报,2003,20(1):31 ~ 38.

[2] 吴文玲．一类广义 Feistel 密码的安全性评估[J]．电子与信息学报,2002,24(9):1177 ~ 1184.

[3] 冯登国,吴文玲．分组密码的设计与分析[M]．北京:清华大学出版社,2000.

[4] Matsui M. Linear Cryptanalysis Method for DES Cipher[R]. In: Advances in Cryptology-Eurocrypt'93, LNCS 765. Springer-Verlag, 1993, 386 - 397.

[5] Chabaud F, Vaudenay S. Links between Differential and Linear Cryptanalysis[R]. Advances in Cryptology-Eurocrypt'94(LNCS No.950), Springer-Verlag, 1995:356 - 365.

[6] Nyberg K. Linear Approximation of Block Ciphers[R]. Advances in Crytology-Eurocrypt'94 (LNCS No. 950), Springer-Verlag, 1995:439 - 444.