一类 Feistel 密码的线性分析 [1]

吕述望 张如文

(中国科学技术大学研究生院信息安全国家重点实验室 北京 100039)

摘 要 该文提出一种新的求取分组密码线性偏差上界的方法，特别适用于密钥线性作用的 Feistel 密码. 该分析方法的思路是，首先对密码体制线性偏差进行严格的数学描述，分别给出密码线性偏差与轮函数 F 及 S 盒的线性偏差的数学关系；然后通过求取线性方程组最小重量解，确定密码线性偏差的上界.

关键词 线性分析，线性偏差表达式，Feistel 密码，轮函数，S 盒

中图号 TN918.1

1 引 言

Feistel 密码是一种迭代密码，由于 DES(Data Encryption Standard) 使用了这种结构而流行. 一个分组长度为 $2e$-bit 的 r 轮迭代 Feistel 密码，如果子密钥与数据的结合方式为模 2 加，则加密过程可以描述为

给定明文 X，记 $X=(X_0,X_1)$，X_0,X_1 的长度为 e-bit . 设 r 个子密钥为 $k_0,k_1,\cdots,k_{r-1}$，则密码的迭代公式为 $X_{i+2}=X_i\oplus F(X_{i+1}\oplus k_i), i=0,1,\cdots,r-1$，密文为 (X_{r+1},X_r). 其中，$\oplus$ 表示模 2 加，F 是 e-bit 输入 e-bit 输出的非线性函数，称为轮函数.

分组密码的安全强度问题非常令人关注，但现代数学的成果还不能完全证明一个密码的安全强度. 通常的做法是考察密码能否抵抗已知密码分析方法的攻击. 目前，线性密码分析 [1] 已成为分组密码设计最为主要的安全性指标之一. 所以，我们应当对分组密码的线性偏差上界做出相对精确的估计，以便在分组密码的设计中对参数选择进行较好的把握.

本文内容安排如下：第 2 节给出一些预备知识；第 3 节给出密码的线性偏差与轮函数线性偏差的数学关系；第 4 节对轮函数具有 SP(Substitution-Permutation) 结构的密码，给出密码的线性偏差与 S 盒线性偏差的数学关系；第 5 节在已有线性偏差表达式的基础上，给出确定线性偏差上界的方法和分析结果.

2 预备知识

定义 1 设 T 是 e-bit 输入 e-bit 输出的非线性变换，即 T: $Z_2^e\to Z_2^e$. 对任意的 W, $V\in Z_2^e$，定义变换 T 的线性偏差为

$$\mathrm{LP}^T(V,W)=2^{-e}\sum_{X\in Z_2^e}(-1)^{(W\cdot X\oplus V\cdot T(X))} \tag{1}$$

定义变换 T 的最大线性偏差为

$$\mathrm{LP}^T_{\max}=\max_{W,V\neq 0}|\mathrm{LP}^T(V,W)| \tag{2}$$

其中 $a\cdot b$ 表示 a 和 b 两个向量的点积，以下简记为 ab. 称 W 为输入线性组合系数，V 为输出线性组合系数.

定理 1 设变换 T 是双射，则

(1) 如果 $W=V=0$，则 $\mathrm{LP}^T(V,W)=1$.

[1] 2002-03-29 收到，2002-11-25 改回

973 项目 (NO.G1999035808) 和 863 项目 (NO.2001AA140101) 资助

(2) 如果 W 和 V 仅有一个为零，则 $\mathrm{LP}^T(V,W)=0$ 。

上述两种情况下的线性偏差只能是 0 或 1 ，我们称其为平凡的。

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，密码的线性偏差记为 $\mathrm{LP}(WX\oplus VK\oplus UY)$ 。

定义 2 对某个置换 T ，如果它的输入、输出线性组合系数均不为零，则称置换 T 是活动的。

定义 3 令 $P:(Z_2^n)^m\to(Z_2^n)^m$ 是一置换，对 $x=(x_1,x_2,\cdots,x_m)\in(Z_2^n)^m$ ， $W_H(x)$ 表示非零的 $x_i(1\le i\le m)$ 的个数，则称 $B_p=\min_{x\neq 0}(W_H(x)+W_H(P(x)))$ 为置换 P 的分支数。

有关文献给出了关于 Feistel 密码线性偏差的上界的一些结论：

结论 1[2] 对于 r 轮迭代的 Feistel 密码，如果其轮函数 F 是双射，且最大线性偏差为 $\mathrm{LP}_{\max}^F$ ，则可对密码的最大线性偏差 $\mathrm{LP}_{\max}$ 做如下估计：

$$\left.\begin{array}{ll}\text{当}r=3n,3n+1\text{时}, & \mathrm{LP}_{\max}\le(\mathrm{LP}_{\max}^F)^{2n}\\ \text{当}r=3n+2\text{时}, & \mathrm{LP}_{\max}\le(\mathrm{LP}_{\max}^F)^{2n+1}\end{array}\right\}\tag{3}$$

结论 2[3] 对于 $4r$ 轮迭代的 Feistel 密码，如果轮函数采用 SP 结构，且混乱层的 S 盒和扩散层的变换 P 都是双射，则线性活动 S 盒个数不小于 $r\times B_p+\lfloor r/2\rfloor$ 。

结论 2 对 $4r$ 轮迭代的 Feistel 密码的最大线性偏差上界做出了估计，但没有给出其他轮迭代的结论，且最少活动 S 盒个数的估计值比较粗。

3 密码线性偏差与轮函数线性偏差的数学关系

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。

在下面的数学推导中我们认为所有的子密钥变量是相互独立、均匀分布的。

设输入 X_0,X_1 ，子密钥 $k_0,\cdots,k_{r-1}$ 是 e-bit 随机变量，由非线性迭代关系：

$$X_{i+2}=X_i\oplus F(X_{i+1}\oplus k_i),\quad i=0,1,\cdots,r-1\tag{4}$$

可以得到 r 轮迭代后的输出 X_r,X_{r+1} 。

当输入 X_0,X_1 ，子密钥 $k_0,\cdots,k_{r-1}$ 和 r 轮迭代后相应的输出 X_r,X_{r+1} 的线性组合系数分别为 $W_0,W_1,V_0,\cdots,V_{r-1},W_r,W_{r+1}$ 时，密码的线性偏差记为

$$\mathrm{LP}(W_0X_0\oplus W_1X_1\oplus V_0k_0\oplus\cdots\oplus V_{r-1}k_{r-1}\oplus W_rX_r\oplus W_{r+1}X_{r+1})\tag{5}$$

首先给出线性偏差的一轮推导关系：

引理 1

$$\begin{aligned}&\mathrm{LP}(W_0X_0\oplus W_1X_1\oplus V_0k_0\oplus\cdots\oplus V_{r-1}k_{r-1}\oplus W_rX_r\oplus W_{r+1}X_{r+1})\\&=\mathrm{LP}^F(W_{r+1},V_{r-1})\mathrm{LP}(W_0X_0\oplus W_1X_1\oplus V_0k_0\oplus\cdots\oplus V_{r-2}k_{r-2}\\&\quad\oplus W_{r+1}X_{r-1}\oplus(V_{r-1}\oplus W_r)X_r)\end{aligned}\tag{6}$$

证明

$$\begin{aligned}
&\mathrm{LP}(W_0X_0 \oplus W_1X_1 \oplus V_0k_0 \oplus \cdots \oplus V_{r-1}k_{r-1} \oplus W_rX_r \oplus W_{r+1}X_{r+1}) \\
&= \alpha \sum_{X_0,X_1,k_0,\cdots,k_{r-1}\in Z_2^e} (-1)^{(W_0X_0\oplus W_1X_1\oplus V_0k_0\oplus\cdots\oplus V_{r-1}k_{r-1}\oplus W_rX_r\oplus W_{r+1}X_{r+1})} \\
&= \alpha \sum_{X_0,X_1,k_0,\cdots,k_{r-1}\in Z_2^e} (-1)^{(W_0X_0\oplus W_1X_1\oplus V_0k_0\oplus\cdots\oplus V_{r-1}k_{r-1}\oplus W_rX_r\oplus W_{r+1}(X_{r-1}\oplus F(X_r\oplus k_{r-1})))} \\
&= \alpha \sum_{X_0,X_1,k_0,\cdots,k_{r-2}\in Z_2^e} (-1)^{(W_0X_0\oplus W_1X_1\oplus V_0k_0\oplus\cdots\oplus V_{r-2}k_{r-2}\oplus W_rX_r\oplus W_{r+1}X_{r-1}\oplus V_{r-1}X_r)} \\
&\quad \times \sum_{k_{r-1}\in Z_2^e} (-1)^{(V_{r-1}(X_r\oplus k_{r-1})\oplus W_{r+1}F(X_r\oplus k_{r-1}))} \\
&= \mathrm{LP}^F(W_{r+1},V_{r-1}) \\
&\quad \times \alpha' \sum_{X_0,X_1,k_0,\cdots,k_{r-2}\in Z_2^e} (-1)^{(W_0X_0\oplus W_1X_1\oplus V_0k_0\oplus\cdots\oplus V_{r-2}k_{r-2}\oplus(W_r\oplus V_{r-1})X_r\oplus W_{r+1}X_{r-1})} \\
&= \mathrm{LP}^F(W_{r+1},V_{r-1})\mathrm{LP}(W_0X_0 \oplus W_1X_1 \oplus V_0k_0 \oplus \cdots \oplus V_{r-2}k_{r-2} \oplus W_{r+1}X_{r-1} \oplus (V_{r-1} \oplus W_r)X_r)
\end{aligned} \tag{7}$$

式中, $\alpha = 2^{-e(r+2)}$, $\alpha' = 2^{-e(r+1)}$ 。　　证毕

由引理 1 可以看到, 经过一轮推导后, 变量 k_{r-1}, X_{r+1} 在公式中消失了。所以, 反复使用上面的引理可以得到如下定理:

定理 2　经过 r 轮迭代, 密码的线性偏差表达式为

(1) 当 r 为偶数, 即 $r = 2m$ 时,

$$\begin{aligned}
&\mathrm{LP}(W_0X_0 \oplus W_1X_1 \oplus V_0k_0 \oplus \cdots \oplus V_{r-1}k_{r-1} \oplus W_rX_r \oplus W_{r+1}X_{r+1}) \\
&\quad = \prod_{i=0}^{m-1} \mathrm{LP}^F(W_r \oplus \sum_{j=i}^{m-1} V_{2j+1}, V_{2i}) \prod_{i=0}^{m-1} \mathrm{LP}^F(W_{r+1} \oplus \sum_{j=i}^{m-2} V_{2j+2}, V_{2i+1}) \\
&\quad\quad \times \mathrm{LP}((W_0 \oplus W_r \oplus \sum_{i=0}^{m-1} V_{2i+1})X_0 \oplus (W_1 \oplus W_{r+1} \oplus \sum_{i=0}^{m-1} V_{2i})X_1)
\end{aligned} \tag{8}$$

(2) 当 r 为奇数, 即 $r = 2m+1$ 时,

$$\begin{aligned}
&\mathrm{LP}(W_0X_0 \oplus W_1X_1 \oplus V_0k_0 \oplus \cdots \oplus V_{r-1}k_{r-1} \oplus W_rX_r \oplus W_{r+1}X_{r+1}) \\
&\quad = \prod_{i=0}^{m} \mathrm{LP}^F(W_{r+1} \oplus \sum_{j=i}^{m-1} V_{2j+1}, V_{2i}) \prod_{i=0}^{m-1} \mathrm{LP}^F(W_r \oplus \sum_{j=i}^{m-1} V_{2j+2}, V_{2i+1}) \\
&\quad\quad \times \mathrm{LP}((W_0 \oplus W_{r+1} \oplus \sum_{i=0}^{m-1} V_{2i+1})X_0 \oplus (W_1 \oplus W_r \oplus \sum_{i=0}^{m} V_{2i})X_1)
\end{aligned} \tag{9}$$

实际上, 在上面的两个表达式中最后一项是线性函数的线性偏差, 由于变量 X_0, X_1 独立均匀分布, 为使整体偏差不为 0 , 其线性组合系数必须为 0 , 即应有

(1) 当 r 为偶数, 即 $r = 2m$ 时, $W_r = W_0 \oplus \sum_{i=0}^{m-1} V_{2i+1}$, $W_{r+1} = W_1 \oplus \sum_{i=0}^{m-1} V_{2i}$;

(2) 当 r 为奇数, 即 $r = 2m+1$ 时, $W_{r+1} = W_0 \oplus \sum_{i=0}^{m-1} V_{2i+1}$, $W_r = W_1 \oplus \sum_{i=0}^{m} V_{2i}$ 。

将以上关系代入 (8), (9) 式中, 则它们的最后一项为 1 , 定理 2 可写为定理 3 的形式。

定理 3　对 r 轮迭代的 Feistel 密码, 其线性偏差表达式为

(1) 当 r 为偶数，即 $r=2m$ 时，

$$\begin{aligned}&\mathrm{LP}(W_0X_0\oplus W_1X_1\oplus V_0k_0\oplus\cdots\oplus V_{r-1}k_{r-1}\oplus W_rX_r\oplus W_{r+1}X_{r+1})\\&=\prod_{i=0}^{m-1}\mathrm{LP}^F(W_0\cdot\sum_{j=0}^{i-1}V_{2j+1},V_{2i})\prod_{i=0}^{m-1}\mathrm{LP}^F(W_1\oplus\sum_{j=0}^{i}V_{2j},V_{2i+1})\end{aligned}\tag{10}$$

且要求输出线性组合系数满足 $W_r=W_0\oplus\sum_{i=0}^{m-1}V_{2i+1}$, $W_{r+1}=W_1\oplus\sum_{i=0}^{m-1}V_{2i}$，否则，密码的线性偏差为零。

(2) 当 r 为奇数，即 $r=2m+1$ 时，

$$\begin{aligned}&\mathrm{LP}(W_0X_0\oplus W_1X_1\oplus V_0k_0\oplus\cdots\oplus V_{r-1}k_{r-1}\oplus W_rX_r\oplus W_{r+1}X_{r+1})\\&=\prod_{i=0}^{m}\mathrm{LP}^F(W_0\cdot\sum_{j=0}^{i-1}V_{2j+1},V_{2i})\prod_{i=0}^{m-1}\mathrm{LP}^F(W_1\oplus\sum_{j=0}^{i}V_{2j},V_{2i+1})\end{aligned}\tag{11}$$

且要求输出线性组合系数满足 $W_{r+1}=W_0\oplus\sum_{i=0}^{m-1}V_{2i+1}$, $W_r=W_1\oplus\sum_{i=0}^{m}V_{2i}$，否则，密码的线性偏差为零。

可以看出，r 轮迭代的 Feistel 密码的线性偏差可以表示为 r 项轮函数 F 线性偏差的乘积，定理 2 和定理 3 是等价的。

4 密码线性偏差与 S 盒线性偏差的数学关系

在 Feistel 密码中，轮函数 F 通常采用 SP 结构，即由混乱层和扩散层两部分构成。混乱层一般由 m 个 $n\times n$ 的 S 盒并置而成，记为非线性变换 t；扩散层一般由可逆的线性变换 P 来实现，记该线性变换矩阵为 A，它是一个 $mn\times mn$ 的矩阵。

设输入变量 $X=(X_1,\cdots,X_m)\in(Z_2^n)^m$，则

$$Y=t(X)=(S(X_1),\cdots,S(X_m)),\quad F(X)=P(t(X))=At(X)=AY\tag{12}$$

对于非线性变换 t 的线性偏差 $\mathrm{LP}^t(v,w)$, 有

定理 4 设 $v=(v_1,\cdots,v_m)$, $w=(w_1,\cdots,w_m)$，其中 v_i, $w_i(i=1,\cdots,m)$ 是 n-bit 变量，则

$$\mathrm{LP}^t(v,w)=\prod_{i=1}^{m}\mathrm{LP}^{\mathrm{S}}(v_i,w_i)\tag{13}$$

定理 5 设轮函数 F 的输入输出线性组合系数分别为 $w,v\in Z_2^{mn}$, 记 $w=(w_1,\cdots,w_m)$, $vA=(v_1,\cdots,v_m)$，则

$$\mathrm{LP}^F(v,w)=\mathrm{LP}^t(vA,w)=\prod_{i=1}^{m}\mathrm{LP}^{\mathrm{S}}(v_i,w_i)\tag{14}$$

定理 5 给出了轮函数 F 的线性偏差与 S 盒的线性偏差之间的数学关系，将该关系代入定理 3 表达式中，不难得出密码的线性偏差由 S 盒的线性偏差表示的数学表达式。r 轮迭代的 Feistel 密码的线性偏差可以表示为 $r\times m$ 项 S 盒线性偏差乘积的形式。

定理 6 r 轮迭代的 Feistel 密码的线性偏差可以表示为

$$\mathrm{LP}(W_0X_0\oplus W_1X_1\oplus W_rX_r\oplus W_{r+1}X_{r+1}\oplus\sum_{i=0}^{r-1}V_ik_i)=\prod_{i=0}^{r-1}\prod_{j=0}^{m-1}\mathrm{LP}^{\mathrm{S}}(v_{ij},w_{ij})\tag{15}$$

其中 v_{ij}, $w_{ij}\in Z_2^n(i=0,1,\cdots,r-1,j=0,1,\cdots,m-1)$ 是线性组合系数 W_0, W_1, V_0, $V_1,\cdots,V_{r-1}$ 的线性组合。

5 确定线性偏差上界算法

算法的基本原理是：由于密码的线性偏差可以分别表示为轮函数 F 线性偏差乘积及 S 盒线性偏差乘积的形式，要使线性偏差取得最大值，需各乘积项中取值为 1 的项数尽可能的多，且不能出现取值为 0 的项。也就是说输入输出线性组合系数均不为零即活动的项数尽可能的少，获得这个项数，令每一项取最大值，就可以得到线性偏差的上界。

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的问题尚无简便的方法，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，用平凡项 (输入输出系数均取 0 的项，即活动项以外的项) 的方程通过初等变换去化简活动项方程，若可将任一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 造成其他项系数必须取 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，则该非 0 项数即为最少活动项数。

下面给出通过实际计算得出的密码线性偏差的上界 $\mathrm{LP}_{\max}$ 与轮函数 F 的线性偏差上界 $\mathrm{LP}^F_{\max}$ 的关系，以及轮函数具有 SP 结构下与 S 盒的线性偏差上界 $\mathrm{LP}^S_{\max}$ 的关系。

5.1 关于轮函数

下面以 6 轮迭代为例对算法的实现给予说明。6 轮迭代密码的线性偏差表达式为

$$\begin{aligned}&\mathrm{LP}(\sum_{i=0}^{1}{}_{\oplus}W_iX_i\oplus\sum_{i=6}^{7}{}_{\oplus}W_iX_i\oplus\sum_{i=0}^{5}{}_{\oplus}V_ik_i)=\\&\quad\mathrm{LP}^F(W_0,V_0)\mathrm{LP}^F(V_0\oplus W_1,V_1)\mathrm{LP}^F(V_1\oplus W_0,V_2)\mathrm{LP}^F(V_0\oplus V_2\oplus W_1,V_3)\\&\quad\times\mathrm{LP}^F(V_1\oplus V_3\oplus W_0,V_4)\mathrm{LP}^F(V_0\oplus V_2\oplus V_4\oplus W_1,V_5)\end{aligned}\tag{16}$$

(16) 式为 6 项轮函数 F 线性偏差的乘积，将其按书写顺序依次记为第 1 项至第 6 项。按照上述方法穷尽，当活动项数为 1, 2, 3 时都出现矛盾。当活动项为 1, 3, 4, 5 这 4 项时没有矛盾，且可以求出组合系数的取值关系：$V_1=V_5=0, W_1=V_0, V_2=V_4$，这时的线性偏差可以表示为 4 项的乘积：$\mathrm{LP}^F(W_0,V_0)\mathrm{LP}^F(W_0,V_2)\mathrm{LP}^F(V_2,V_3)\mathrm{LP}^F(W_0\oplus V_3,V_2)$。可以看到这时表达式中的变量只有 4 个。由此可见，活动轮函数 F 最少项数为 4，可得：$\mathrm{LP}_{\max}\le(\mathrm{LP}^F_{\max})^4$。

同样的方法，可以求出任意 r 轮迭代最少活动轮函数 F 项数 $\mathrm{AN}^F_{\min}$。结果如表 1 所示。可以看出，该结果与结论 1 给出的估计值是一致的。

表 1　最少活动轮函数 F 项数 $\mathbf{AN}^F_{\min}$

轮数 r	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\mathrm{AN}^F_{\min}$	3	4	4	5	6	6	7	8	8	9	10	10	11	12
轮数 r	19	20	21	22	23	24	25	26	27	28	29	30	31	32
$\mathrm{AN}^F_{\min}$	12	13	14	14	15	16	16	17	18	18	19	20	20	21

5.2 关于 S 盒

定理 6 将密码的线性偏差表示为多项 S 盒线性偏差乘积的形式，我们可以利用类似前面所述方法求取最少活动 S 盒个数。略有不同的是，S 盒的平凡项是输入或输出组合系数的 n 个 bit 全部为 0 的项，其余为活动项。

我们以 64bit 的 Feistel 密码为例，给出部分最少活动 S 盒个数的结果。假设轮函数的混乱层采用 4 个并置的 8 进 8 出的 S 盒，扩散层选用可逆的线性变换 P。

下面针对两种不同的线性变换 P，分别给出相应的最少活动 S 盒个数 $\mathrm{AN}^S_{\min}$。

(1) 线性变换 P 为：$P(X)=X\oplus(X<<<8)\oplus(X<<<16)$，其中 $X\in Z_2^{32}$，$<<<$ 表示左循环移位。该线性变换的分支数为 4，最少活动 S 盒个数结果如表 2 所示。该结果显然优于利用结论 2 中由分支数估计的最少活动 S 盒个数。

表 2 最少活动 S 盒个数 $AN^S_{\min}$

轮数 r	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$AN^S_{\min}$	6	8	8	10	12	12	14	16	16	18	20	20	22	24
轮数 r	19	20	21	22	23	24	25	26	27	28	29	30	31	32
$AN^S_{\min}$	24	26	28	28	30	32	32	34	36	36	38	40	40	42

(2) 线性变换 P 为： $P(X) = X \oplus (X <<< 6) \oplus (X <<< 14) \oplus (X <<< 22) \oplus (X <<< 24)$，其中 $X \in Z_2^{32}$，$<<<$ 表示左循环移位。该线性变换的分支数为 5，最少活动 S 盒个数结果如表 3 所示。该结果与利用结论 2 中由分支数估计的最少活动 S 盒个数基本一致，但略优。

表 3 最少活动 S 盒个数 $\mathrm{AN}^S_{\min}$

轮数 r	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\mathrm{AN}^S_{\min}$	6	7	8	11	12	13	14	17	18	19	20	23	24	25
轮数 r	19	20	21	22	23	24	25	26	27	28	29	30	31	32
$\mathrm{AN}^S_{\min}$	26	29	30	31	32	35	36	37	38	41	42	43	44	47

从以上两个结果可以看到，结论 2 利用分支数对最少活动 S 盒个数的估计结果是没有错误的，但不精确，所以应当具体问题具体分析。

参 考 文 献

[1] M. Matsui, Linear cryptanalysis method for DES ciper, Advances in Cryptology-Eurocrypt'93, Berlin: Springer- Verlag, 1993, 386–397.

[2] M. Kanda, Y. Takashima, T. Matsumoto, A strategy for constructing fast round function with practical security against differential and linear cryptanalysis, Selected Areas in Cryptography, Lecture Notes of Computer Science 1556, Springer-Verlag, 1999, 264–279.

[3] M. Kanda, Practical security evaluation against differential and linear attacks for Feistel ciphers with SPN round function, Selected Areas in Cryptography, Lecture Notes of Computer Science 2012, Springer-Verlag, 2000, 324–338.

LINEAR CRYPTANALYSIS FOR A CLASS OF FEISTEL CIPHERS

Lü Shuwang Zhang Ruwen

(*State Key Laboratory of Information Security, Graduate School, University of Science and Technology of China, Beijing* 100039, *China*)

Abstract In this paper, a new method is proposed for seeking the upper bounds of maximum linear bias for block ciphers, which is especially applicable to a class of Feistel ciphers that key is XORed with data. This technique consists of two steps. Firstly, the mathematical relationship between linear bias of ciphers and linear bias of round function F and S-box respectively is given by carrying out strictly mathematical expression of linear bias for ciphers. Next, the upper bounds of linear bias for ciphers are determined by seeking the solution with minimum weight for linear equation group. Using this method the upper bounds of linear bias within 32 rounds are given.

Key words Linear cryptanalysis, Linear bias expression, Feistel ciphers, Round function, S-box

吕述望： 男，1941 年生，教授，博士生导师，研究方向为信息安全技术研究.

张如文： 男，1967 年生，副研究员，硕士生，研究方向为信息安全技术研究.