一、基本思路

线性密码分析是一种已知明文攻击——攻击者已知密钥相同的多组明密文对，求解密钥。与选择明文攻击或选择密文攻击相比，攻击者无法任意选择一段明文或密文，获得对应的密文或明文。

线性密码分析的思路是分析明文和密文之间的线性表达式成立的概率。其中明密文之间的线性表达式为：

$$Xi1 \oplus Xi2 \oplus \cdots \oplus Xiu \oplus Yj1 \oplus Yj2 \oplus \cdots \oplus Yjv = 0$$

其中 Xi 表示的是输入中的第 i 个 bit,Yj 表示的是输出中的第 j 的 bit。这个表达式不是必然成立的， 对于一个优秀的密码算法，它成立的概率应当是 1/2 ， 即左边的结果可能为 0 ，也可能为 1 。如果该表达式成立的概率距离 1/2 越远，则越容易使用线性分析法，获得明密文之间的线性关系，从而通过多组明密文对分析出密钥的值。假设线性表达式成立的概率为 P，那么 |P-1/2| 越大，越容易受到线性密码分析攻击。

在本文中，我们分析了一个输入(明文)，和输出(第 4 轮轮密钥异或的结果)的线性逼近。

二、S 盒分析

设一个 S 盒如下

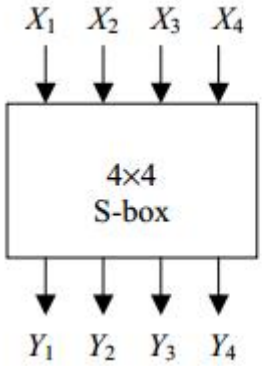

Figure 2. S-box Mapping

对于此 S 盒进行分析，求解公式 X2⊕X3⊕=Y1⊕Y3⊕Y4 的概率可得如下图。求得偏差为 0

X_1	X_2	X_3	X_4	Y_1	Y_2	Y_3	Y_4	$X_2 \oplus X_3$	$Y_1 \oplus Y_3 \oplus Y_4$	$X_1 \oplus X_4$	Y_2	$X_3 \oplus X_4$	$Y_1 \oplus Y_4$
0	0	0	0	1	1	1	0	0	0	0	1	0	1
0	0	0	1	0	1	0	0	0	0	1	1	1	0
0	0	1	0	1	1	0	1	1	0	0	1	1	0
0	0	1	1	0	0	0	1	1	1	1	0	0	1
0	1	0	0	0	0	1	0	1	1	0	0	0	0
0	1	0	1	1	1	1	1	1	1	1	1	1	0
0	1	1	0	1	0	1	1	0	1	0	0	1	0
0	1	1	1	1	0	0	0	0	1	1	0	0	1
1	0	0	0	0	0	1	1	0	0	1	0	0	1
1	0	0	1	1	0	1	0	0	0	0	0	1	1
1	0	1	0	0	1	1	0	1	1	1	1	1	0
1	0	1	1	1	1	0	0	1	1	0	1	0	1
1	1	0	0	0	1	0	1	1	1	1	1	0	1
1	1	0	1	1	0	0	1	1	0	0	0	1	0
1	1	1	0	0	0	0	0	0	0	1	0	1	0
1	1	1	1	0	1	1	1	0	0	0	1	0	1

Table 3. Sample Linear Approximations of S-box

对所有 256 个公式进行偏差分析可得如下结果

		Output Sum															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Input Sum	0	+8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	0	0	−2	−2	0	0	−2	+6	+2	+2	0	0	+2	+2	0	0
	2	0	0	−2	−2	0	0	−2	−2	0	0	+2	+2	0	0	−6	+2
	3	0	0	0	0	0	0	0	0	+2	−6	−2	−2	+2	+2	−2	−2
	4	0	+2	0	−2	−2	−4	−2	0	0	−2	0	+2	+2	−4	+2	0
	5	0	−2	−2	0	−2	0	+4	+2	−2	0	−4	+2	0	−2	−2	0
	6	0	+2	−2	+4	+2	0	0	+2	0	−2	+2	+4	−2	0	0	−2
	7	0	−2	0	+2	+2	−4	+2	0	−2	0	+2	0	+4	+2	0	+2
	8	0	0	0	0	0	0	0	0	−2	+2	+2	−2	+2	−2	−2	−6
	9	0	0	−2	−2	0	0	−2	−2	−4	0	−2	+2	0	+4	+2	−2
	A	0	+4	−2	+2	−4	0	+2	−2	+2	+2	0	0	+2	+2	0	0
	B	0	+4	0	−4	+4	0	+4	0	0	0	0	0	0	0	0	0
	C	0	−2	+4	−2	−2	0	+2	0	+2	0	+2	+4	0	+2	0	−2
	D	0	+2	+2	0	−2	+4	0	+2	−4	−2	+2	0	+2	0	0	+2
	E	0	+2	+2	0	−2	−4	0	+2	−2	0	0	−2	−4	+2	−2	0
	F	0	−2	−4	−2	−2	0	+2	0	0	−2	+4	−2	−2	0	+2	0

Table 4. Linear Approximation Table

三、具体实现

依据书中的提示可得如下执行图

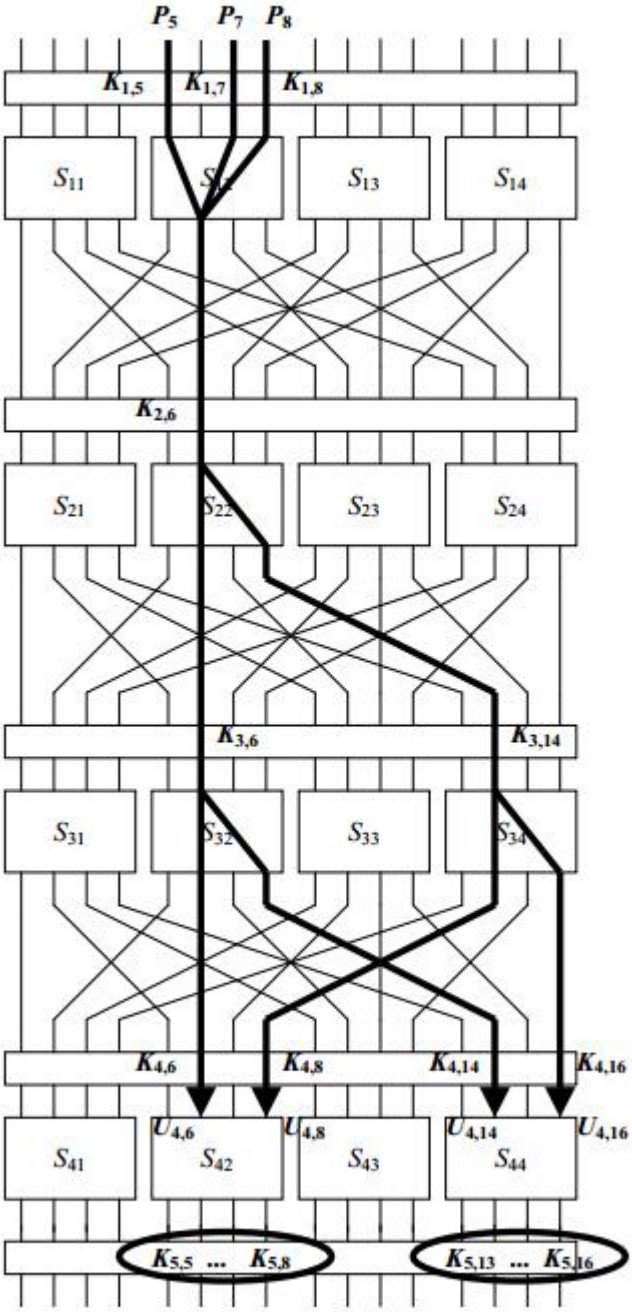

Figure 3. Sample Linear Approximation

对于要求解的部分，共有 256 种可能性，因此我们需要对这 256 个可能的密钥进行依次尝试。由于堆积引理，我们只需要记录 U4,6⊕U4,8⊕U4,14⊕U4,16⊕P5⊕P7⊕P8=0 时的次数就，最后计算概率即可得出相应的 KEY。而剩余位的密钥也只需暴力求解即可。