

	Y1	Y2	Y3	Y4
X1	-2	0	2	0
X2	-2	-2	-2	0
X3	2	-2	2	0
X4	0	0	0	0

Looking at the S\_box biases we observe that the following equations hold with a bias  $\pm \frac{1}{8}$

1.  $x_1 \oplus y_1 = 0$
2.  $x_1 \oplus x_3 = 0$
3.  $x_2 \oplus y_1 = 0$
4.  $x_2 \oplus y_2 = 0$
5.  $x_2 \oplus y_3 = 0$
6.  $x_3 \oplus y_1 = 0$
7.  $x_3 \oplus y_2 = 0$
8.  $x_3 \oplus y_3 = 0$

We can use these to construct the following linear trail->

Round 1

$$X_{11} \oplus Y_{11} = 0$$

$$X_{21} \oplus Y_{21} = 0$$

$$X_{31} \oplus Y_{31} = 0$$

$$\text{Where } X_{21} = K_{21} \oplus Y_{11}, X_{31} = K_{31} \oplus Y_{21}, X_{41} = K_{41} \oplus Y_{31}$$

Combining all these and using the pumping lemma

$$X_{11} \oplus Y_{11} \oplus K_{21} \oplus Y_{11} \oplus Y_{21} \oplus K_{31} \oplus Y_{21} \oplus Y_{31} = 0$$

$$\text{i.e. } P_1 \oplus X_{41} = 0$$

with a probability

$$= \frac{1}{2} + 2^2 \left(\frac{1}{8}\right)^3$$

$$\text{i.e. a bias} = \frac{1}{128}$$

Thus for the first 6 S\_boxes we have the following trails

1. Box 1  
 $P_1 \rightarrow X_{1,1} \rightarrow Y_{1,1} \rightarrow X_{2,1} \rightarrow Y_{2,1} \rightarrow X_{3,1} \rightarrow Y_{3,1} \rightarrow X_{4,1}$   
 $\text{i.e. } P_1 \oplus X_{4,1} = 0$
2. Box 2  
 $P_9 \rightarrow X_{1,9} \rightarrow Y_{1,9} \rightarrow X_{2,3} \rightarrow Y_{2,3} \rightarrow X_{3,17} \rightarrow Y_{3,17} \rightarrow X_{4,5}$   
 $\text{i.e. } P_9 \oplus X_{4,5} = 0$
3. Box 3  
 $P_{17} \rightarrow X_{1,17} \rightarrow Y_{1,17} \rightarrow X_{2,5} \rightarrow Y_{2,5} \rightarrow X_{3,2} \rightarrow Y_{3,2} \rightarrow X_{4,9}$   
 $P_{17} \oplus X_{4,9} = 0$
4. Box 4  
 $P_{25} \rightarrow X_{1,25} \rightarrow Y_{1,25} \rightarrow X_{2,7} \rightarrow Y_{2,7} \rightarrow X_{3,18} \rightarrow Y_{3,18} \rightarrow X_{4,13}$
5. Box 5  
 $P_2 \rightarrow X_{1,2} \rightarrow Y_{1,2} \rightarrow X_{2,9} \rightarrow Y_{2,9} \rightarrow X_{3,3} \rightarrow Y_{3,3} \rightarrow X_{4,17}$   
 $P_2 \oplus X_{4,17} = 0$
6. Box 6  
 $P_{10} \rightarrow X_{1,10} \rightarrow Y_{1,10} \rightarrow X_{2,11} \rightarrow Y_{2,11} \rightarrow X_{3,19} \rightarrow Y_{3,19} \rightarrow X_{4,21}$

$$P_{10} \oplus X_{4,21} = 0$$

No linear trails could be obtained for boxes 7 and 8.

As the bias for each trail is  $1/128$ , we need to have at least  $128^2$  pairs