



[ASSIGNMENT #1]



OCTOBER 4, 2021

[MHAMOUD SAMI]

[MOHAMED ABOHELAL]

Firstly, we generated a random S-box and its inverse.

```
sbox = {0:0x2, 1:0x1, 2:0xE, 3:0x7, 4:0x4, 5:0xa, 6:0x8, 7:0xD, 8:0xf, 9:0xc, 0xA:0x9, 0xB:0x0, 0xC:0x3, 0xD:0x5, 0xE:0x6, 0xF:0xb}
sbox_inv = {0x2:0, 0x1:1, 0xE:2, 0x7:3, 0x4:4, 0xa:5, 0x8:6, 0xD:7, 0xf:8, 0xc:9, 0x9:0xA, 0x0:0xB, 0x3:0xC, 0x5:0xD, 0x6:0xE, 0xb:0xF}
```

Figure 1 generating an s-box S

Secondly, we constructed its Linear Approximation Table.

```
Linear Approximation Table for basic SPN cipher's sbox:
(x-axis: output equation - 8, y-axis: input equation - 8)
08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 02 -2 00 00 -2 02 00 00 02 -2 00 00 -2 -6 00
00 00 00 00 00 00 -4 -4 02 -2 02 -2 02 -2 -2 02
00 -2 -2 04 00 02 -2 00 02 04 00 02 02 00 00 -2
00 00 00 00 00 00 04 -4 00 00 00 00 04 04 00 00
00 -2 -2 -4 00 02 -2 00 -4 02 02 00 00 02 -2 00
00 00 00 00 00 00 00 00 -2 02 -2 -6 02 -2 02 -2
00 02 -2 00 00 06 02 00 02 00 00 -2 -2 00 00 02
00 02 00 -2 00 02 00 -2 00 -2 00 02 00 -2 00 -6
00 04 02 02 00 00 -2 02 00 00 02 -2 00 04 -2 -2
00 02 00 -2 04 -2 00 -2 02 04 02 00 -2 00 02 00
00 00 02 -2 -4 00 -2 -2 02 02 -4 00 -2 02 00 00
00 -2 -4 -2 00 -2 00 02 04 -2 00 -2 00 02 00 -2
00 04 -2 -2 00 00 -2 02 00 00 -2 02 04 00 02 02
00 -2 04 -2 04 02 00 02 02 00 -2 00 02 00 -2 00
00 00 -2 02 04 00 -2 -2 -2 -2 -4 00 -2 02 00 00
```

Figure 2 linear approximation table

Thirdly, we found the best Linear Approximation.

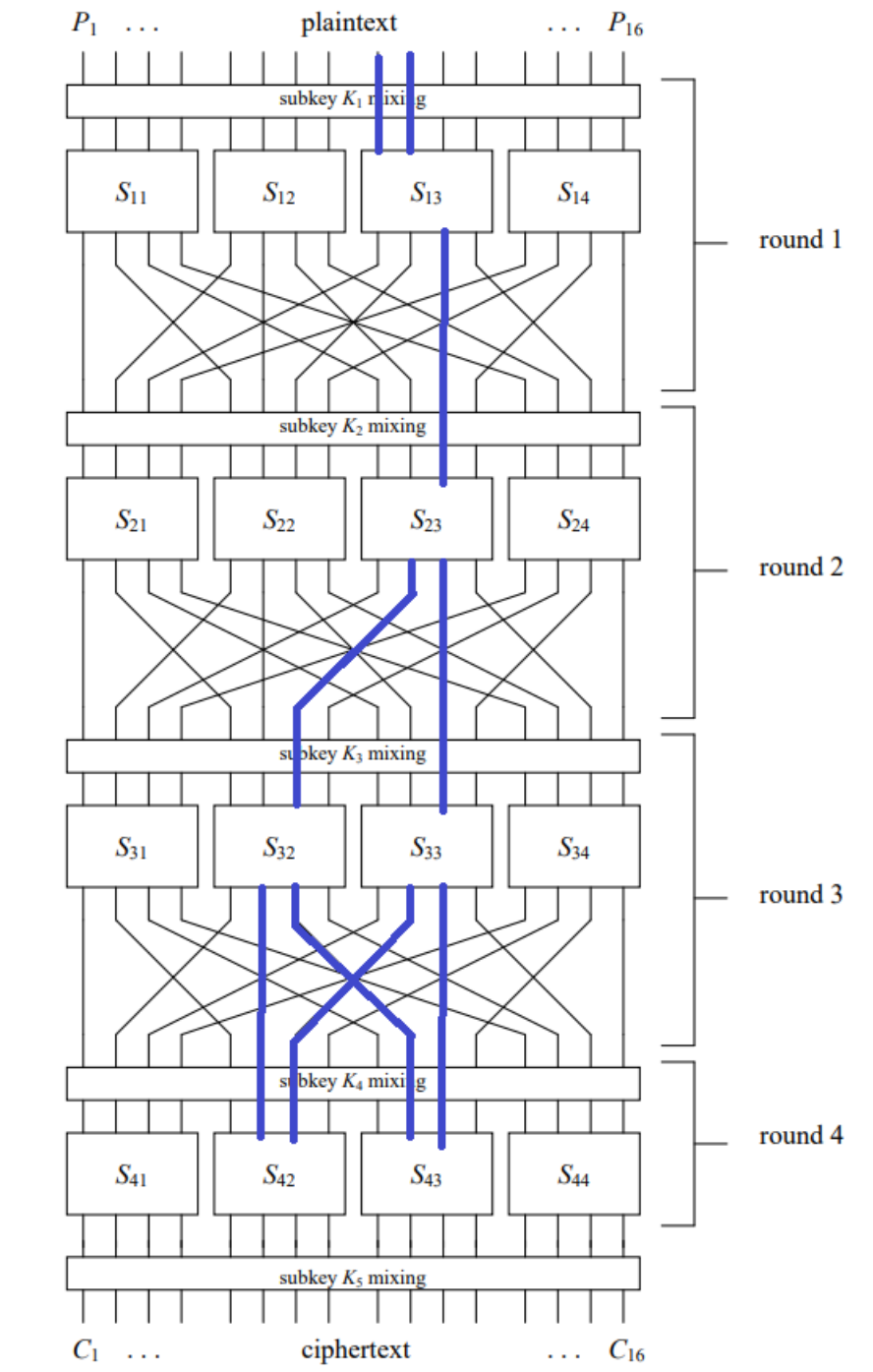


Figure 3 Linear approximation path

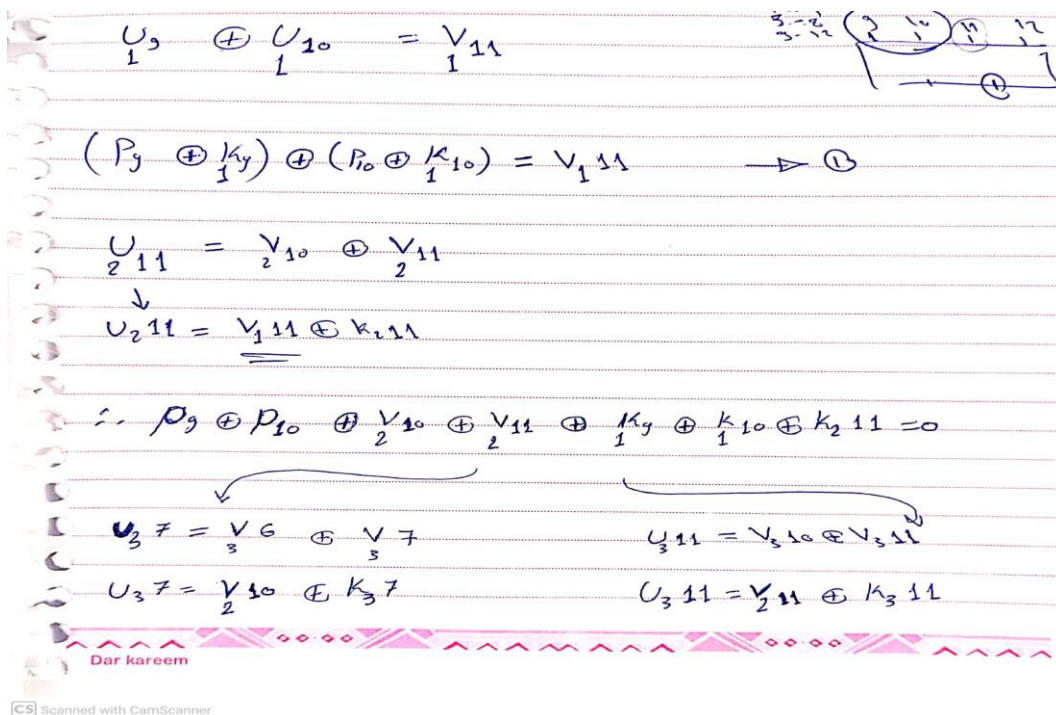
The next step, we calculated the bias of the path we have chosen.

$$x_1 \oplus x_2 = y_2 \longrightarrow \text{round 1}$$

$$x_3 = y_2 \oplus y_3 \longrightarrow \text{round 2}$$

$$x_3 = y_2 \oplus y_3 \longrightarrow \text{round 3}$$

$$x_3 = y_2 \oplus y_3 \longrightarrow \text{round 3}$$



Handwritten mathematical derivation for a cryptanalysis problem, showing the calculation of a bias for a chosen path. The derivation involves XOR operations on variables U , V , and K across multiple rounds, leading to a final equation $U_3 11 = V_2 11 \oplus K_3 11$.

$$U_1 3 \oplus U_1 10 = V_1 11$$

Diagram illustrating a path selection process with nodes 9, 10, 11, 12 and a highlighted path from 9 to 10 to 11.

$$(P_9 \oplus K_1 9) \oplus (P_{10} \oplus K_1 10) = V_1 11 \rightarrow \textcircled{1}$$

$$U_2 11 = V_2 10 \oplus V_2 11$$

$$\downarrow$$

$$U_2 11 = V_1 11 \oplus K_2 11$$

$$\therefore P_9 \oplus P_{10} \oplus V_2 10 \oplus V_2 11 \oplus K_1 9 \oplus K_1 10 \oplus K_2 11 = 0$$

$$U_3 7 = V_3 6 \oplus V_3 7$$

$$U_3 11 = V_3 10 \oplus V_3 11$$

$$U_3 7 = V_2 10 \oplus K_3 7$$

$$U_3 11 = V_2 11 \oplus K_3 11$$

Dar kareem

Scanned with CamScanner

$$V_3 6 \oplus V_3 7 \oplus V_2 10 \oplus K_3 7 \oplus V_3 10 \oplus V_3 11 \oplus V_2 11 \oplus K_3 11 = 0 \rightarrow \textcircled{2}$$

① and ②

$$P_9 \oplus P_{10} \oplus V_3 6 \oplus V_2 11 \oplus K_3 7 \oplus K_3 10 \oplus K_2 11$$

$$\oplus V_3 6 \oplus V_3 7 \oplus V_3 10 \oplus V_3 11 \oplus V_2 11 \oplus K_3 7 \oplus K_3 11 = 0$$

$$P_9 \oplus P_{10} \oplus V_3 6 \oplus V_3 7 \oplus V_3 10 \oplus V_3 11 \oplus K_3 7 \oplus K_3 10 \oplus K_2 11 \oplus K_3 7 \oplus K_3 11 = 0$$

(A)

$$U_4 6 = V_3 6 \oplus K_4 6$$

$$U_4 7 = V_3 10 \oplus K_4 7$$

$$U_4 10 = V_3 7 \oplus K_4 10$$

$$U_4 11 = V_3 11 \oplus K_4 11$$

$$\therefore P_9 \oplus P_{10} \oplus U_4 6 \oplus U_4 7 \oplus U_4 10 \oplus U_4 11 + \sum K = 0$$

we will use BJT (S₄₂, S₄₃)

- Probability = $\frac{1}{2} - 2^3 \left(\frac{1}{4} - \frac{1}{2} \right)^4$

- Bias = -1/32

By application of the Piling-Up Lemma, the above expression holds with probability $15/32$ (that is, with a bias of $-1/32$).

Now since ΣK is fixed, we note that must hold with a probability of either $15/32$ or $(1-15/32) = 17/32$, depending on whether $\Sigma K = 0$ or 1 , respectively. In other words, we now have a linear approximation of the first three rounds of the cipher with a bias of magnitude $1/32$.

The last step, we extracted the key bits.

We would try all 256 values for the target partial subkey $[K_5,5 \dots K_5,12]$

```
Test key k = dc75ea2a15969750067c (k_5 = 0x67c).  
Target partial subkey K_5,5...k_5,8 = 0b0110 = 0x6  
Target partial subkey K_5,9...k_5,12 = 0b0111 = 0x7  
Testing each target subkey value...  
Highest bias is 0.0398 for subkey value 0x67.  
Success!
```

Discuss the results of the attacks.

After trying all 256 values for the target partial subkey we found that highest bias is 0.0398 for subkey value 0x67. And we can conclude that we can get the whole key of the encryption And of course we can't depend on the S-P-N or DES for encrypting our Data.

Our code to attack the SPN network

- [GitHub - Mahmoudsami11095/Crypto](#)

References

- <https://github.com/hkscy/Basic-SPN-cryptanalysis>
- https://ioactive.com/wp-content/uploads/2015/07/ldc_tutorial.pdf