CS666-ASSIGNMENT - 4

Name: Kakumanu Vamsee Krishna

Roll no: 22111065

Group Details: Group No. 3

Kakumanu Vamsee Krishna (22111065)
Rumit Gore (22111409)
Sandula Lavanya (22111078)
Aditya Kankriya (22111072)
Pratik Patil (22111047)

Python Tool Version used: 3.9.12(Spyder-Anaconda)

Question:

In this assignment, you have to implement a Differential Fault Attack on AES. You would be supplied with two pairs of faulty and correct ciphertext and using that you need to recover the first column (first 32 bits) of the round 10 key. The two pairs of faulty and correct ciphertext for each group are as given below:

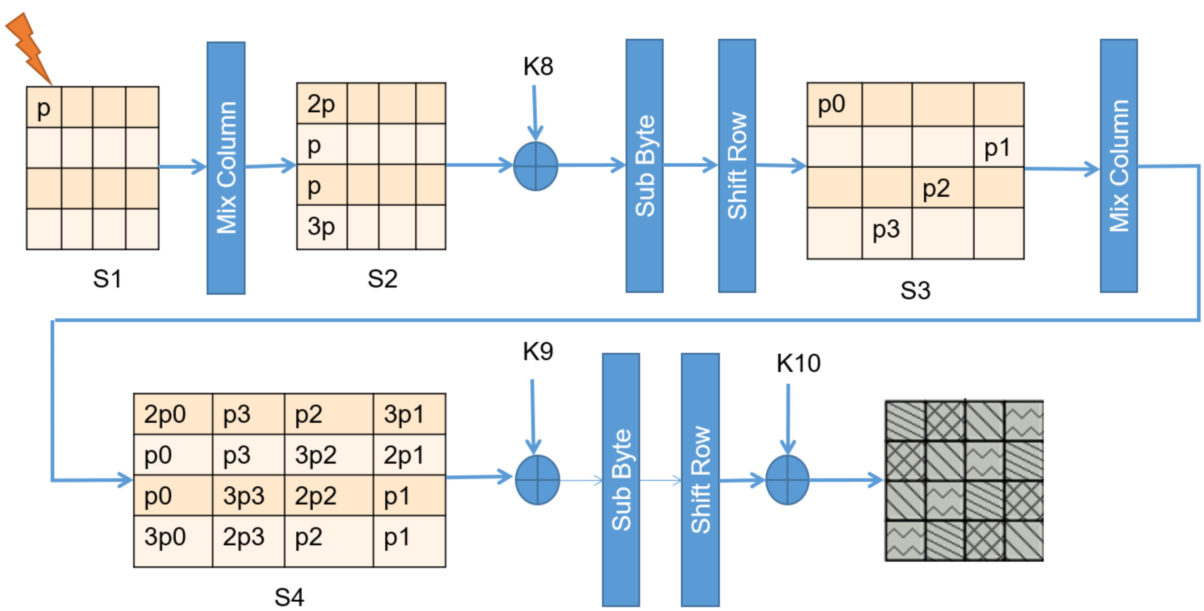
Group 3:

Correct Ciphertext1:
0x317982fa5666677f86b021f313e21725
Correct Ciphertext2:
0xeeade76ae853cceca45dddfe257c63c0

Faulty Ciphertext1:
0x77f3dac61758cdb2cd9ab5d532d4ec8d
Faulty Ciphertext2:
0x0c1531c070f9303ef23fca1f5bab1007

Logic:

The faults are assumed to be introduced before the MixColumn of round 8. So, the propagation of fault across various subsequent rounds of AES is shown in the image below.



The above image shows the propagation of fault when the fault is introduced in the first byte of the 8^{th} round AES.

So, the idea is to introduce 4 different faults at 4 different locations to get 16 equations. Solution to these 16 equations will give the entire 128-bit key of the 10^{th} round of AES.

Notations:

C - Correct Ciphertext

C^* - Faulty Ciphertext

f - Fault

S^{-1} - Inverse Sub-box

So, firstly introducing fault at (0,0) before the 8^{th} round MixColumn operation, this fault propagates in (0,0) (1,3) (2,2) (3,1) after MixColumn operation and AddRoundKey of 9^{th} round, these 4 faults further propagate all over the AES box after MixColumn and AddRoundKey of 9^{th} round, so we will have 16 equations out of which four will correspond to 1 fault, such for 4 faults we have 16 equations

For fault at (0,0) we get following 4 equations:

$$2p0 = S^{-1}(C_{0,0} \oplus K_{0,0}) \oplus S^{-1}(C^*_{0,0} \oplus K_{0,0})$$

$$p0 = S^{-1}(C_{1,3} \oplus K_{1,3}) \oplus S^{-1}(C^*_{1,3} \oplus K_{1,3})$$

$$p0 = S^{-1}(C_{2,2} \oplus K_{2,2}) \oplus S^{-1}(C^*_{2,2} \oplus K_{2,2})$$

$$3p0 = S^{-1}(C_{3,1} \oplus K_{3,1}) \oplus S^{-1}(C^*_{3,1} \oplus K_{3,1})$$

For fault at (3,1) we get following 4 equations:

$$p3 = S^{-1}(C_{0,1} \oplus K_{0,1}) \oplus S^{-1}(C^*_{0,1} \oplus K_{0,1})$$

$$p3 = S^{-1}(C_{1,0} \oplus K_{1,0}) \oplus S^{-1}(C^*_{1,0} \oplus K_{1,0})$$

$$3p3 = S^{-1}(C_{2,3} \oplus K_{2,3}) \oplus S^{-1}(C^*_{2,3} \oplus K_{2,3})$$

$$2p3 = S^{-1}(C_{3,2} \oplus K_{3,2}) \oplus S^{-1}(C^*_{3,2} \oplus K_{3,2})$$

For fault at (2,2) we get following 4 equations:

$$p2 = S^{-1}(C_{0,2} \oplus K_{0,2}) \oplus S^{-1}(C^*_{0,2} \oplus K_{0,2})$$

$$3p2 = S^{-1}(C_{1,1} \oplus K_{1,1}) \oplus S^{-1}(C^*_{1,1} \oplus K_{1,1})$$

$$2p2 = S^{-1}(C_{2,0} \oplus K_{2,0}) \oplus S^{-1}(C^*_{2,0} \oplus K_{2,0})$$

$$p2 = S^{-1}(C_{3,3} \oplus K_{3,3}) \oplus S^{-1}(C^*_{3,3} \oplus K_{3,3})$$

For fault at (1,3) we get following 4 equations:

$$\mathbf{3p1 = S^{-1} (C_{0,3} \oplus K_{0,3}) \oplus S^{-1} (C^{*}_{0,3} \oplus K_{0,3})}$$

$$\mathbf{2p1 = S^{-1} (C_{1,2} \oplus K_{1,2}) \oplus S^{-1} (C^{*}_{1,2} \oplus K_{1,2})}$$

$$\mathbf{p1 = S^{-1} (C_{2,1} \oplus K_{2,1}) \oplus S^{-1} (C^{*}_{2,1} \oplus K_{2,1})}$$

$$\mathbf{p1 = S^{-1} (C_{3,0} \oplus K_{3,0}) \oplus S^{-1} (C^{*}_{3,0} \oplus K_{3,0})}$$

Now, the overall approach is to solve the above 16 sets of equations to get the complete 128-bits of round 10 key out of which the first 32-bits required can be easily calculated by solving for the guessed key and fault, obtain the probable list of keys for both faulty ciphertexts and having a intersection of both those lists will give the correct key.

<u>Answer:</u>

The total 128-bits of 10th round key found is =

0x ade208dd 380df400 7b37a576 e918ed66

Hence, the first 32-bits of 10th round key =

0x ade208dd

Output:

```
----final key---
 OrderedDict([(0, '0xad'), (1, '0xe2'), (2, '0x8'), (3, '0xdd'), (4,
'0x38'), (5, '0xd'), (6, '0xf4'), (7, '0x0'), (8, '0x7b'), (9, '0x37'),
(10, '0xa5'), (11, '0x76'), (12, '0xe9'), (13, '0x18'), (14, '0xed'),
(15, '0x66')])
```

Website Referred to check whether the 10th round key generated is correct or not by using the Master Key,

(0x 02a21a3ccdd2223ff75128421d1af222) which was provided:

https://www.cryptool.org/en/cto/aes-step-by-step

```
Key
02a21a3c  cdd2223f  f7512842  1d1af222

Expanded Key
02a21a3c  cdd2223f  f7512842  1d1af222  a12b8998  6cf9aba7  9ba883e5  86b271c7  94884fdc  f871e47b  63d9679e  e56b1659  efcf8405
17be607e  746707e0  910c11b9  194dd284  0ef3b2fa  7a94b51a  eb98a4a3  4f04d86d  41f76a97  3b63df8d  d0fb7b2e  6025e91d  21d2838a
1ab15c07  ca4a2729  f6e94c69  d73bcfe3  cd8a93e4  07c0b4cd  cc64f1ac  1b5f3e4f  d6d5adab  d1151966  8eb0c292  95effcdd  433a5176
922f4810  ade208dd  380df400  7b37a576  e918ed66
```