**CS666-ASSIGNMENT - 4**

**Group Details:** Group No. 7

Shrawan Kumar (22111080)  
Haris Khan (22111026)  
Subhajit Panday (22111058)

**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 7**:

Correct Ciphertext1: 0x5ac34223b23627e417ff32d15dc62b3a

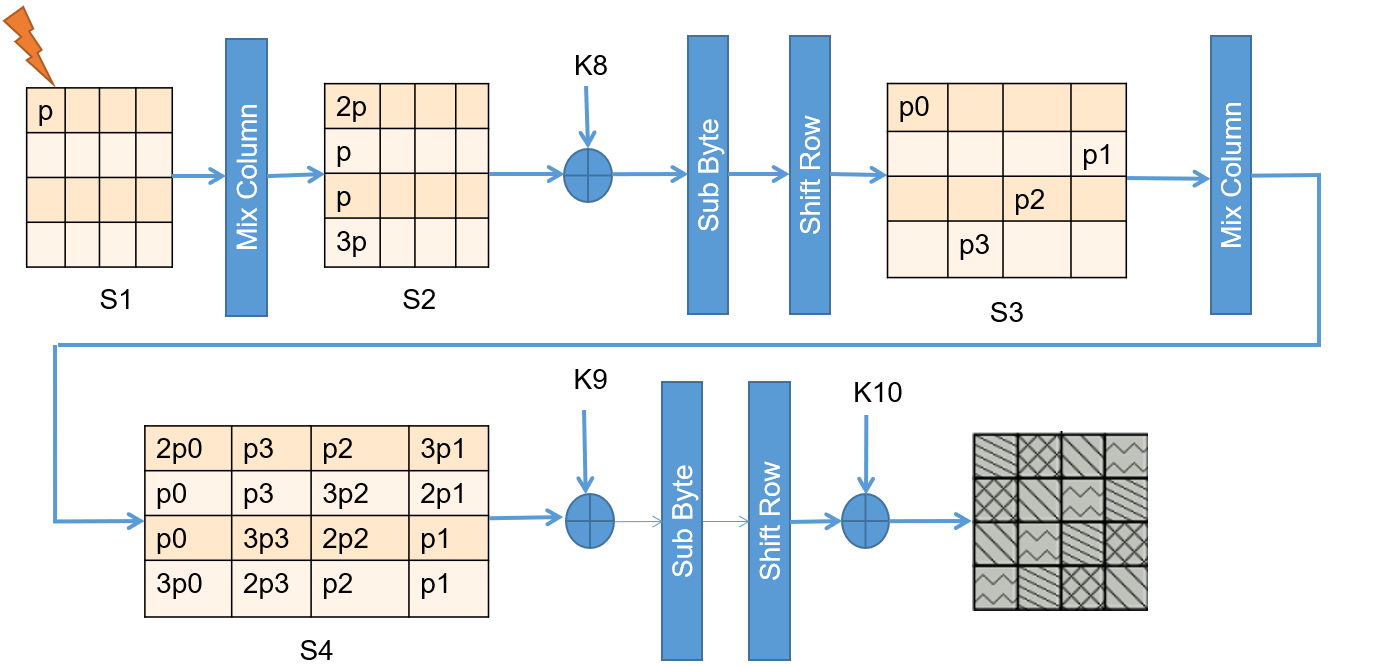
Correct Ciphertext2: 0x620f470b13743f5f9f1026a0eed920eb

Faulty Ciphertext1: 0xf4cc767bbddd6637aebd12ed264f360e

Faulty Ciphertext2: 0xea9403be8583cd160ff038e449701213

**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 8th 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 10th 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 8th round MixColumn operation, this fault propagates in (0,0) (1,3) (2,2) (3,1) after MixColumn operation and AddRoundKey of 9th round, these 4 faults further propagate all over the AES box after MixColumn and AddRoundKey of 9th 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 (C0,0 ⊕ K0,0) ⊕ S-1 (C\*0,0 ⊕ K0,0)**

**p0 = S-1 (C1,3 ⊕ K1,3) ⊕ S-1 (C\*1,3 ⊕ K1,3)**

**p0 = S-1 (C2,2 ⊕ K2,2) ⊕ S-1 (C\*2,2 ⊕ K2,2)**

**3p0 = S-1 (C3,1 ⊕ K3,1) ⊕ S-1 (C\*3,1 ⊕ K3,1)**

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

**p3 = S-1 (C0,1 ⊕ K0,1) ⊕ S-1 (C\*0,1 ⊕ K0,1)**

**p3 = S-1 (C1,0 ⊕ K1,0) ⊕ S-1 (C\*1,0 ⊕ K1,0)**

**3p3 = S-1 (C2,3 ⊕ K2,3) ⊕ S-1 (C\*2,3 ⊕ K2,3)**

**2p3 = S-1 (C3,2 ⊕ K3,2) ⊕ S-1 (C\*3,2 ⊕ K3,2)**

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

**p2 = S-1 (C0,2 ⊕ K0,2) ⊕ S-1 (C\*0,2 ⊕ K0,2)**

**3p2 = S-1 (C1,1 ⊕ K1,1) ⊕ S-1 (C\*1,1 ⊕ K1,1)**

**2p2 = S-1 (C2,0 ⊕ K2,0) ⊕ S-1 (C\*2,0 ⊕ K2,0)**

**p2 = S-1 (C3,3 ⊕ K3,3) ⊕ S-1 (C\*3,3 ⊕ K3,3)**

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

**3p1 = S-1 (C0,3 ⊕ K0,3) ⊕ S-1 (C\*0,3 ⊕ K0,3)**

**2p1 = S-1 (C1,2 ⊕ K1,2) ⊕ S-1 (C\*1,2 ⊕ K1,2)**

**p1 = S-1 (C2,1 ⊕ K2,1) ⊕ S-1 (C\*2,1 ⊕ K2,1)**

**p1 = S-1 (C3,0 ⊕ K3,0) ⊕ S-1 (C\*3,0 ⊕ K3,0)**

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.

**Answer:**

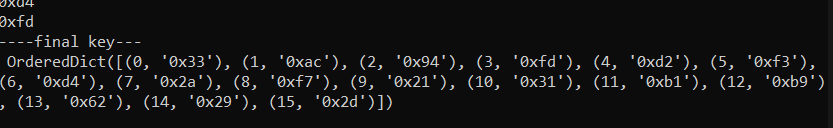
The total 128-bits of 10th round key found is =

**0x 33ac94fd d2f3d42a f72131b1 b962292d**

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

**0x 33ac94fd**

**Output:**

****

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

**(0x 8521142aadd100662714583cedeea133)** which was provided:

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

