Assignment 3 SPM 2022 Report

Prasanna Bartakke EE19B106

September 18, 2022

8^{th} round attack on AES

The ciphertext and the corresponding faulty ciphertext are represented as follows:

$$CT = \begin{pmatrix} x_0 & x_4 & x_8 & x_{12} \\ x_1 & x_5 & x_9 & x_{13} \\ x_2 & x_6 & x_{10} & x_{14} \\ x_3 & x_7 & x_{11} & x_{15} \end{pmatrix}, FCT = \begin{pmatrix} x_0^{'} & x_4^{'} & x_8^{'} & x_{12}^{'} \\ x_1^{'} & x_5^{'} & x_9^{'} & x_{13}^{'} \\ x_2^{'} & x_6^{'} & x_{10}^{'} & x_{14}^{'} \\ x_3^{'} & x_7 & x_{11} & x_{15}^{'} \end{pmatrix}$$

The 10^{th} round key, K_{10} is represented as:

$$K_{10} = \begin{pmatrix} k_0 & k_4 & k_8 & k_{12} \\ k_1 & k_5 & k_9 & k_{13} \\ k_2 & k_6 & k_{10} & k_{14} \\ k_3 & k_7 & k_{11} & k_{15} \end{pmatrix}$$

The following figure shows the propagation of fault assuming that a fault was induced in the first byte in the 8^{th} round of AES.

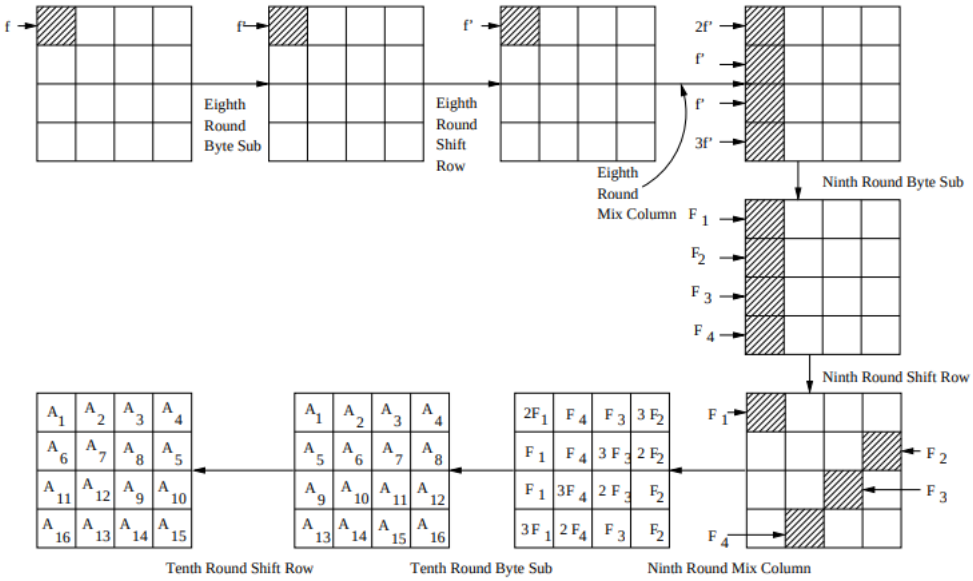

Fig. 1: Propagation of Fault Induced in the input of eighth round of AES.

We can see that a single fault induced in the 8^{th} diffuses in all the bytes by the end of the 10^{th} round. Considering the state of the difference after the ninth round shift rows, the following equations are obtained:

$$2\delta_1 = S^{-1}(x_0 \oplus k_0) \oplus S^{-1}(x_0^{'} \oplus k_0)$$

$$\delta_1 = S^{-1}(x_{13} \oplus k_{13}) \oplus S^{-1}(x_{13}^{'} \oplus k_{13})$$

$$\delta_1 = S^{-1}(x_{10} \oplus k_{10}) \oplus S^{-1}(x_{10}^{'} \oplus k_{10})$$

$$3\delta_1 = S^{-1}(x_7 \oplus k_7) \oplus S^{-1}(x_7^{'} \oplus k_7)$$

Where $\delta_1, k_0, k_{13}, k_{10}, k_7$ are unknown values $\in \{0, 1, ..., 255\}$. All these values are guessed and the number of possibilities for these 32 bits of the key are reduced by selecting values which satisfy the equations. For a given value of δ_1 the values of k_0, k_{13}, k_{10}, k_7 that satisfy all the equations simultaneously are noted down using 4 different exhaustive searches.

Similarly, we can form the remaining equations to reduce the search space for the remaining set of bytes. Following are the required equations:

For $(x_4, x_1, x_{14}, x_{11})$

$$3\delta_2 = S^{-1}(x_4 \oplus k_4) \oplus S^{-1}(x_4^{'} \oplus k_4)$$

$$2\delta_2 = S^{-1}(x_1 \oplus k_1) \oplus S^{-1}(x_1^{'} \oplus k_1)$$

$$\delta_2 = S^{-1}(x_{14} \oplus k_{14}) \oplus S^{-1}(x_{14}^{'} \oplus k_{14})$$

$$\delta_2 = S^{-1}(x_{11} \oplus k_{11}) \oplus S^{-1}(x_{11}^{'} \oplus k_{11})$$

For (x_8, x_5, x_2, x_{15})

$$\delta_3 = S^{-1}(x_8 \oplus k_8) \oplus S^{-1}(x_5^{'} \oplus k_5)$$

$$3\delta_3 = S^{-1}(x_5 \oplus k_5) \oplus S^{-1}(x_5^{'} \oplus k_5)$$

$$2\delta_3 = S^{-1}(x_2 \oplus k_2) \oplus S^{-1}(x_2^{'} \oplus k_2)$$

$$\delta_3 = S^{-1}(x_{15} \oplus k_{15}) \oplus S^{-1}(x_{15}^{'} \oplus k_{15})$$

For (x_{12}, x_9, x_6, x_3)

$$\delta_4 = S^{-1}(x_{12} \oplus k_{12}) \oplus S^{-1}(x_{12}^{'} \oplus k_{12})$$

$$\delta_4 = S^{-1}(x_9 \oplus k_9) \oplus S^{-1}(x_9^{'} \oplus k_9)$$

$$3\delta_4 = S^{-1}(x_6 \oplus k_6) \oplus S^{-1}(x_6^{'} \oplus k_6)$$

$$2\delta_4 = S^{-1}(x_3 \oplus k_3) \oplus S^{-1}(x_3^{'} \oplus k_3)$$

Each set of 4 bytes of K_{10} returns 2^8 unique hypothesis for those bytes. Thus, assuming that the fault was induced in the first byte, a single pair of ciphertext and faulty ciphertext can give 2^{32} unique hypothesis for the 10^{th}round key. As we do not know where the fault was induced, we can induce faults in the remaining columns, and get the key hypothesis corresponding to those faults. Following is the analysis of the offline analysis on the first pair of ciphertext and faulty ciphertext.

Number of candidates for positions 0, 13, 10, 7: 976 4, 1, 14, 11: 976 8, 5, 2, 15: 1232 12, 9, 6, 3: 1008 Using 1 ct-fct pairs, total number of candidates for 10th RK are: 1182962221056

We can see that more pairs are needed to get a single key hypothesis. We do the same analysis for the second pair of ciphertext and faulty ciphertext, and take the intersection of the two sets of hypothesis.

```
Pair 1
Number of candidates for positions
0, 13, 10, 7: 976
4, 1, 14, 11: 976
8, 5, 2, 15: 1232
12, 9, 6, 3: 1008
Using 1 ct-fct pairs, total number of candidates for 10th RK are: 1182962221056
Pair 2
Number of candidates for positions
0, 13, 10, 7: 1
4, 1, 14, 11: 1
8, 5, 2, 15: 1
12, 9, 6, 3: 1
Using 2 ct-fct pairs, total number of candidates for 10th RK are: 1
```

Thus, **using two pairs, we can recover the 10^{th} round key**. The 10^{th} round key obtained is:

```
10th round key: d9 ec 45 68 9a 0b 2c e3 86 2d 0b de c6 04 09 ba
```

As we have 4 pairs of ciphertext and faulty ciphertext, the result was verified on all combinations of two pairs, and the same key was obtained from all combinations. The master key and remaining round keys can be recovered by the inverse key scheduling from the 10^{th} round key. The results are stored in the file roundkeys.txt. The time required to recover the 10^{th} round key is **5 seconds**.

```
Master key(round key 0): a1 1a bb 9e 20 0f 61 52 de 26 fe 59 f2 1f 87 69
```

References

1. https://eprint.iacr.org/2009/575.pdf