CS666: Hardware Security and IOT

Assignment 4

Group 1 :
SOHAM GHOSAL (180771)
TARUN KANODIA (190902)
TUSHAR SINGLA (190918)
AYUSH SHAKYA (180178)

Introduction

This assignment required the group to perform a DFA attack on AES when we are provided with 2 pairs each of correct and incorrect ciphertext. The objective is to obtain/recover first 32 bits of the K-10 key (10th round key). The approach we took while solving this assignment is detailed below:

- We find 4 bytes of the 10th round key in one go. This can be done using relations like the one listed below:

$$
\begin{aligned}
2p_0 &= S^{-1}\left(C_{0,0} \oplus K^{10}_{0,0}\right) \oplus S^{-1}\left(C^*_{0,0} \oplus K^{10}_{0,0}\right) \\
p_0 &= S^{-1}\left(C_{3,1} \oplus K^{10}_{3,1}\right) \oplus S^{-1}\left(C^*_{3,1} \oplus K^{10}_{3,1}\right) \\
p_0 &= S^{-1}\left(C_{2,2} \oplus K^{10}_{2,2}\right) \oplus S^{-1}\left(C^*_{2,2} \oplus K^{10}_{2,2}\right) \\
3p_0 &= S^{-1}\left(C_{1,3} \oplus K^{10}_{1,3}\right) \oplus S^{-1}\left(C^*_{1,3} \oplus K^{10}_{1,3}\right)
\end{aligned}
$$

- Our algorithm creates two sets, set 1 of possible keys using equations 1 and 2, and another set 2 of possible keys using equations 3 and 4.
- Finally, we try all the possibilities for the keys using a cross of these two sets and satisfy all four equations by them to yield the set of possible 4 bytes of the 10th round key.
- We repeat the above 2 steps for the second pair of correct and faulty ciphertexts provided, and obtain yet another set of possible 4 bytes (at the same position as previous step) of the 10th round key.
- The intersection of these two sets correctly determines the 4 bytes at the corresponding positions.
- The above four steps are repeated for the remaining 12 bytes of the key(3 more times), using other fault equations (present in code).

This output of our code would fetch us the correct value of the 10th round key.

Data Provided (Group 1):

- **Correct Ciphertext1**: 0xd8fdc9b896a929cb33df86b634e0dc04
- **Correct Ciphertext2**: 0xaa5e77e2064d15e14babd14f5feafa77
- **Faulty Ciphertext1**: 0x32622c1f5deed912b18a59996444273f
- **Faulty Ciphertext2**: 0xb7565eced22c123b2d6e2fc9101d2315

Equations: These equations find one key byte from each column one at a time.

$$\begin{aligned}
2p_0 &= S^{-1}\left(C_{0,0} \oplus K_{0,0}^{10}\right) \oplus S^{-1}\left(C_{0,0}^{*} \oplus K_{0,0}^{10}\right)\\
p_0 &= S^{-1}\left(C_{3,1} \oplus K_{3,1}^{10}\right) \oplus S^{-1}\left(C_{3,1}^{*} \oplus K_{3,1}^{10}\right)\\
p_0 &= S^{-1}\left(C_{2,2} \oplus K_{2,2}^{10}\right) \oplus S^{-1}\left(C_{2,2}^{*} \oplus K_{2,2}^{10}\right)\\
3p_0 &= S^{-1}\left(C_{1,3} \oplus K_{1,3}^{10}\right) \oplus S^{-1}\left(C_{1,3}^{*} \oplus K_{1,3}^{10}\right)
\end{aligned}$$

$$\begin{aligned}
p_1 &= S^{-1}\left(C_{1,0} \oplus K_{1,0}^{10}\right) \oplus S^{-1}\left(C_{1,0}^{*} \oplus K_{1,0}^{10}\right)\\
p_1 &= S^{-1}\left(C_{0,1} \oplus K_{0,1}^{10}\right) \oplus S^{-1}\left(C_{0,1}^{*} \oplus K_{0,1}^{10}\right)\\
3p_1 &= S^{-1}\left(C_{3,2} \oplus K_{3,2}^{10}\right) \oplus S^{-1}\left(C_{3,2}^{*} \oplus K_{3,2}^{10}\right)\\
2p_1 &= S^{-1}\left(C_{2,3} \oplus K_{2,3}^{10}\right) \oplus S^{-1}\left(C_{2,3}^{*} \oplus K_{2,3}^{10}\right)
\end{aligned}$$

$$p_2 = S^{-1}\left(C_{2,0} \oplus K^{10}_{2.0}\right) \oplus S^{-1}\left(C^*_{2,0} \oplus K^{10}_{2,0}\right)$$
$$3p_2 = S^{-1}\left(C_{1,1} \oplus K^{10}_{1,1}\right) \oplus S^{-1}\left(C^*_{1,1} \oplus K^{10}_{1,1}\right)$$
$$2p_2 = S^{-1}\left(C_{0,2} \oplus K^{10}_{0,2}\right) \oplus S^{-1}\left(C^*_{0,2} \oplus K^{10}_{0,2}\right)$$
$$p_2 = S^{-1}\left(C_{3,3} \oplus K^{10}_{3,3}\right) \oplus S^{-1}\left(C^*_{3,3} \oplus K^{10}_{3,3}\right)$$

$$3p_3 = S^{-1}\left(C_{3,0} \oplus K^{10}_{3,0}\right) \oplus S^{-1}\left(C^*_{3,0} \oplus K^{10}_{3,0}\right)$$
$$2p_3 = S^{-1}\left(C_{2,1} \oplus K^{10}_{2,1}\right) \oplus S^{-1}\left(C^*_{2,1} \oplus K^{10}_{2,1}\right)$$
$$p_3 = S^{-1}\left(C_{1,2} \oplus K^{10}_{1,2}\right) \oplus S^{-1}\left(C^*_{1,2} \oplus K^{10}_{1,2}\right)$$
$$p_3 = S^{-1}\left(C_{0,3} \oplus K^{10}_{0,3}\right) \oplus S^{-1}\left(C^*_{0,3} \oplus K^{10}_{0,3}\right)$$

Since we require first 4 bytes of the 10th round key, we ultimately have to obtain all the 16 bytes of the key from the above equations.

Conclusions

The key found by above algorithm is: **0xCDD6088CDCBDCFFF2ECF793A96FEE199.** The 10th round key obtained from the initial key (present in the file "keys.txt" at the assignment page) after applying key expansion algorithm is: **0xCDD6088CDCBDCFFF2ECF793A96FEE199,** which matches the key found by our algorithm.

References

The **AES code** provided in Assignment 3 has been used as the boilerplate code as a starting point in our assignment 4 as well.