Assignment No. 3

CS666: Hardware Security for Internet of Things

Instructions

1. Even though you are working in a group, you need to submit solutions individually.
2. The solution for the assignment should be submitted as a zip file. The file should be named as `StudentNameRollNumber.zip`.
3. The submission should contain the following:
   - A Python file.
   - The report (as a PDF).

Questions

1. You will be provided with the power traces of AES. The power traces are stored in a CSV file, where each row indicates the power consumption of one AES execution. For every row, the first entry is plaintext, the second entry is ciphertext, and all the subsequent entries are power consumption values. Your task is to write a code for Difference of Mean Attack, and use that code on the given power traces to recover the 4th and 5th bytes of the secret key used in the AES execution. You will be provided with 5 CSV files, you have to use one according to your group number. (e.g., if your group number is 1, then use HW power trace 1.csv)
2. 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. *If the size of your encrypted message (ciphertext) is less than 16 bytes, add a '0' at the beginning.* The two pairs of faulty and correct ciphertext for each group are as given below:
   - **Group 1:**
     - Correct Ciphertext1: `0xd8fdc9b896a929cb33df86b634e0dc04`
     - Correct Ciphertext2: `0xaa5e77e2064d15e14babd14f5feafa77`
     - Faulty Ciphertext1: `0x32622c1f5deed912b18a59996444273f`
     - Faulty Ciphertext2: `0xb7565eced22c123b2d6e2fc9101d2315`
   - **Group 2:**
     - Correct Ciphertext1: `0xb21eeb73953e7a2771db222ecbeea788`
     - Correct Ciphertext2: `0xcabe3e9988d6666a96a39e7b659ca91`
     - Faulty Ciphertext1: `0x33cf60141fd2f121ff9a6126fefd03e6`
     - Faulty Ciphertext2: `0x92317b8a9e24f1960f37385a4085b0d5`
   - **Group 3:**

  - Correct Ciphertext1: `0x317982fa5666677f86b021f313e21725`
  - Correct Ciphertext2: `0xeeade76ae853cceca45dddfe257c63c0`
  - Faulty Ciphertext1: `0x77f3dac61758cdb2cd9ab5d532d4ec8d`
  - Faulty Ciphertext2: `0xc1531c070f9303ef23fca1f5bab1007`
- **Group 4:**
  - Correct Ciphertext1: `0x6559ddd4dde1df14a4888fb98dde1e67`
  - Correct Ciphertext2: `0x7bde21b7f4a53022be2788696816249`
  - Faulty Ciphertext1: `0xf289ba7cea98d64fa982fe226f4bdf48`
  - Faulty Ciphertext2: `0x488a3c55b75ba66f857ca45b6ad47335`
- **Group 5:**
  - Correct Ciphertext1: `0xcb9e460f86b40b7d3b9ec48a0726acef`
  - Correct Ciphertext2: `0xe38830724a96247185621d21458c16fb`
  - Faulty Ciphertext1: `0x7fb5bd33e30867882ad89d326d824dc9`
  - Faulty Ciphertext2: `0x48c3b33b3516a1f8c31d08f90479b7b5`