Introduction to Hardware Security

Assignment 1

Due Date: August 3, 2022 (11:59 PM)

General Instructions:

- This will be a group assignment. Every group consists of six members. You can create your group as per your convenience. The only restriction is that each group should contain at most six members.
- Only electronic submissions will be accepted.
- Late submissions will have penalties.
- Any sort of plagiarism will be penalised. If you are referring to any materials online or books, please cite them accordingly otherwise it will be considered as plagiarism.
- Please submit a detailed report explaining how you have solved the assignment.

Question

In this assignment, you will be provided with the power consumption of the last round of AES. The power traces are obtained from SAKURA-G platform that runs an implementation of AES-128 on a Spartan-6 FPGA. The power trace is 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 Correlation Power Attack, and use that code on the given power trace to recover the target byte assigned to your group. The target byte assignment for the groups are given below:

- Group 1: 1st byte
- Group 2: 2nd byte
- Group 3: 3rd byte
- Group 4: 5th byte
- Group 5: 6th byte
- Group 6: 7th byte
- Group 7: 9th byte
- Group 8: 10th byte

- Group 9: 11th byte
- Group 10: 13th byte

An example code that obtains the 0th byte of the key is provided for your reference. We would like to thank Prof. Debdeep Mukhopadhyay of IIT Kharagpur for kindly providing us the power traces of FPGA based AES implementation.

Deliverables:

1. Even though you are working in 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 StudentName_RollNumber.zip. You also need to submit a text file where your group members' roll numbers and names will be listed.
3. The submission should contain the following:
    - A python file.
    - The report (as pdf).
    - A text file containing your group information.