Assignment 2 SPM 2022 (July-Nov)

Power Analysis (100 Marks)

Deadline: September 3rd, 2022

In class, we saw the Correlation Power Analysis (CPA)/ Difference of Mean (DOM) attacks on AES where we collect power traces from ChipWhisperer running AES encryption to find the key. You can find the implementation for the same here. Each of the teams is provided with a similar power trace here for CLEFIA-128 T-Table implementation for different keys. You need to figure out the following from the power traces

1. The round keys used in the first round in the Encryption function for your given key i.e. RK0, RK1. **(16 marks)**
2. The round keys used in the last round (round 18) in the Encryption function for your given key i.e. RK34, RK35. **(16 marks)**
3. The round keys for the second round masked by the whitening keys i.e. (RK2 ⊕ WK0) and (RK3 ⊕ WK1) used in the Encryption function for your given key. **(16 marks)**
4. Submit a report explaining the changes made to the template code provided and the methodology used (DOM/CPA) to identify the keys. Mention the power model used (Hamming weight/Hamming Distance) for your analysis. Also provide an analysis of relation between the confidence in the key and the number of traces available. **(52 marks)**
