Project 4: CPA on AES-128

The goal of the project is to launch Correlation Power Analysis attack on AES-128 and recover the round key used in the last round.

Similar to the DPA project, your CPA attack will focus on the operations in the10^{th} round. The power consumption you will exploit is for updating register with the ciphertext at the end of the 10^{th} round. The number of transitions decides how much power is consumed at that moment. In DPA, you attempt to find power differences between transition and no transition at one bit location each time. In CPA, you will exploit the correlation between the number of transitions (considering all bit locations in a byte) and the power consumption.

You will be using the same data set as in Project 3. And you should have already got the correct key through DPA.

Deliverables:

- Launch CPA attack using cipher text and the corresponding power traces provided, and then guess the round keys in 10_{th} round. Compare them with the results in your DPA attack.
- Compare the effectiveness of CPA and DPA attacks.
- Improve your DPA report and incorporate your CPA approach and results in the report.