Resources on Power Analysis and Fault Attacks

Preparation Lecture 6

- Study the DES cipher specification, including the internal components of its round function (sboxes, addround key, expansion, permutation).

- Watch an introductory video on Side-channel Analysis:
  https://www.youtube.com/watch?v=OlX-p4AGhWs

Literature Lecture 6

- Read the full process of Correlation Power Analysis (CPA) in Sections 6.1 and 6.2:
  Differential Power Analysis, Chapter 6 on Power Analysis Attacks - Revealing the Secrets of Smart Cards by S. Mangard et al.

- Read the full Differential Fault Analysis process:
  Differential Fault Analysis of DES by M. Rivain
  https://tinyurl.com/2s3krvdy
  Make sure that you are familiar with the DES reminder in section 3.2 and then focus on the attack on the 16th round in section 3.3.1