Project 2

Differential Power Analysis of AES

Project Due: Thursday, November 26, 23:59

Compulsory Project

The goal of this project is to perform the differential power analysis of the AES.
You are given the power consumption traces as measured on the microcontroler ATmega16 during a S-box computatation in the first round of the AES for different inputs (which are provided in a separate file). Note that those are NOT 16 different S-boxes. It is just ONE S-box corresponding to a particular byte position in the data state of the AES. So there is only one fixed secret byte of key material involved into the computation, which is added to the input before the S-box computation.
Your task is to recover this secret key byte using the differential power analysis.

About the Data

You will receive two files with the data you need to perform the attack: TX.dat and inputsX.dat, where X is an integer representing the data set you have been given.
The file TX.dat contains the T matrix c.f. the slides in lecture 8, i.e. the N power traces. In this case, $N = 600$ and each trace has $t = 55$ samples, i.e. T is a 60055 matrix. The format of TX.dat is such that line i of the file corresponds to row i of T, and each value in the row of T is separated by a comma in a line of the file. The file inputsX.dat contains one line with comma separated values. Each value is a number between 0 and 255 (both included). There are $N = 600$ values in total, and the ith value corresponds to the plaintext byte used for the ith power trace (ith row) of the matrix T.

Your Task

Your hand-in (via CampusNet) should include:

1. source code of your power analysis implementation,
2. the recovered key byte value, and
3. a short report.

Group work is strongly encouraged in Project 2 but please make sure to hand in individually.