Exercise Sheet 4

Differential Power Analysis

Obligatory homework this week: Exercise 5. Hand-in by October 24, 23:59.

Exercise 1: Power consumption of a 4-bit bus
Assume that the power is consumed by the bus when its wire's value is changed from 0 to 1 and from 1 to 0. Consider a 4-bit bus consisting of 4 parallel wires. The value v on the bus is changed to value u. Consider the current 4-bit value $v = (v_3v_2v_1v_0)_2$ and the new 4-bit value $u = (u_3u_2u_1u_0)_2$ on this 4-bit bus. Derive a dependency on the power consumption of this operation on the values u and v.

Exercise 2: Power consumption of a 4-bit bus precharged to all ones
Consider the bus of the previous exercise. Assume that it is precharged to a constant value (all ones) before a new value v is written on this bus. Derive a dependency on the power consumption of this operation on the values u and v.

Exercise 3: Pure power leakage of the PRESENT S-box
Consider the 4-bit PRESENT S-box:

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S[x]$	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

Assume that the power consumed by the device implementing PRESENT is proportional to the Hamming weight of S-box output. Assume the secret key value of $0xB$ and produce the HW-simulated power consumption traces for 50 random plaintext nibbles. Feel free to use computer and C (or a computer algebra system) for this task.

Exercise 4: DPA on PRESENT with simulated traces
Given the 50 simulated power consumption traces of the previous exercise perform the DPA attack based on correlation coefficient as explained in the lecture. Feel free to use any kind of computer assistance here - from using it as a calculator to writing a dedicated program. How would your results change for a larger number of traces? How would you results change for traces that contain some noise?

Exercise 5: DPA on AES
The goal of this exercise 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.
You will receive two files with the data you need to perform the attack: TX.dat and inputsX.dat, *where X is the least significant digit of your study number*.

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 600×55 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 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, but please make sure to hand in individually.