Lab 3
Side Channels

Due: September 27, 2022

1 DPA: Introduction and Goals

The purpose of this assignment is to provide a hands-on introduction to power-based side-channel analysis. You are given a set of power traces of a smart-card executing AES-ECB operations and the associated input/output values of AES, and you are asked to extract the 128-bit secret key via Differential Power Analysis (DPA).

1. input_plaintext.txt
2. output_ciphertext.txt
3. power_traces.csv

These files correspond to 10000 AES-ECB executions with random input and a fixed, secret key. Hence, there are 10000 distinct input values, corresponding output values, and power measurements. input_plaintext.txt is the set of 128-bit input plaintexts of AES, output_plaintext.txt is the set of 128-bit output ciphertext for AES, and power_traces.csv contain the power measurement for each input-output pair.

2 Problem 1: Analyze the power trace

Figure 2 Plot the first power trace in the power_traces.csv file and analyze it.
Question 1: What do the peaks in the power trace correspond to? Why are there 11 power peaks and what is happening at each power peak?

3 Problem 2: Perform the DPA attack

Let's execute the DPA attack.
Question 2:What is an easy target operation for DPA? Describe how many bits of the key your DPA attack estimate at a time. Hint: You are given the input, think of the very first operation of AES.
Apply DPA on the first byte of the key, plot correlation results **Figure 3** for all 256 key guesses.
Find the maximum correlation among key guesses (consider both positive and negative peaks) and plot the two best key guesses, on the same figure, **Figure 4** that have the maximum correlation.
Question 3: Which one is the correct key guess? Why do you see these two results?
Question 4: Which point in the time domain has the maximum power leak (ie. correlation)? Plot the "evolution" of correlation coefficient for all 256 key guesses for 10000 measurements at this particular time instance **Figure 5**.
Question 5: Starting at how many traces, does the correct key guess show highest correlation?
Question 6: Apply DPA on the entire key, write the value of the 128-bit AES key.

4 Problem 3: Analyze the DPA attack

Question 7: What is the mean time to disclosure, ie. the number of traces required to extract the key?
Question 8: Compare this with the theoretical crypto-analysis of AES, what is the reduction ratio in the number of traces required to break AES? What is the reason for this reduction?
Bonus1: Describe a simple pre-processing on power traces that will improve their alignment, and hence the DPA attack efficiency.
Bonus2: Assume that you do not have access to input plaintext but only to output ciphertext, how would you modify the attack?

5 Graded Items

You will turn in a hard copy report of your results as well as any code to the TA on Canvas. Make sure to include answers to every question as well as the following figures in the report.

1. Figure 1 Plot of the first power trace.

2. Figure 2 Plot of the correlation of all key guesses for the first-byte of AES key.

3. Figure 3 Plot of two best key guesses.

4. Figure 4 Plot of the "evolution" of all key guesses for 10000 measurements at this particular time instance.

Lab reports must be in readable English and not raw dumps of log-files. Your lab reports must be typed and must not exceed 6 pages. You are encouraged to use the report template provided on Canvas. Please submit your lab report and all of your code in a zip/tar file on on Canvas as lab2_EID.tar.gz or lab2_EID.zip.