Supplementary Exercise Sheet

Differential Power Analysis - Extra Exercises

Exercise 1: Data Requirement for DPA
Consider the DPA you did on AES-128 in Exercise 5 from Exercise Sheet 4. Here, you recovered one key byte using 600 traces.
Consider the case where you sort the list of 256 key guesses by the maximum absolute correlation. If you have sufficient traces, the correct key will be at the top of the list. Now, decrease the number of traces, and check the ranking of the correct key byte. How few traces can you use and still have the correct key at the top of the list? Do you get the same number for all 10 key bytes?

Exercise 2: AES-128 Key Recovery
Using the data for the 10 key bytes you have received as a representative data set, how many traces do you need on average to have all 16 bytes of a full AES-128 key at the top of their respective lists?

Exercise 3: Data/Time Trade-Off
Consider the following data/time trade-off: Instead of using enough traces for all 16 key bytes to have the highest rank, we use fewer traces, but keep the k most likely key values for each byte.

- How many possible 128-bit keys do we obtain, using this method?
- How would you check if a possible key is correct?
- The DTU Compute cluster has nodes with two Intel Xeon Processor E5-2680 processors, each with 10 cores. Under optimal conditions, such a node can perform approximately 2^{51} AES-128 encryptions in a month. Using this kind of computational power, how few traces can you use, and still recover the encryption key?