Modern Cryptology - DPA on AES

Anders Lammert Hartmann (s153596)

Amalie Due Jensen (s160503)

March 12, 2021

1 Introduction

In this assignment we will perform a cryptographic side channel attack - more specifically a differential power analysis with a hamming weight model - on AES trying to find a certain byte of the AES-key. We will write a program in C able to perform the attack and present the found (and hopefully correct) key byte for two different data sets. The implementation and a description of how to use our implementation can be found on `https://github.com/AmalieDue/AES_differential_power_analysis`.

2 Description of attack

For the attack we will be using to data sets:

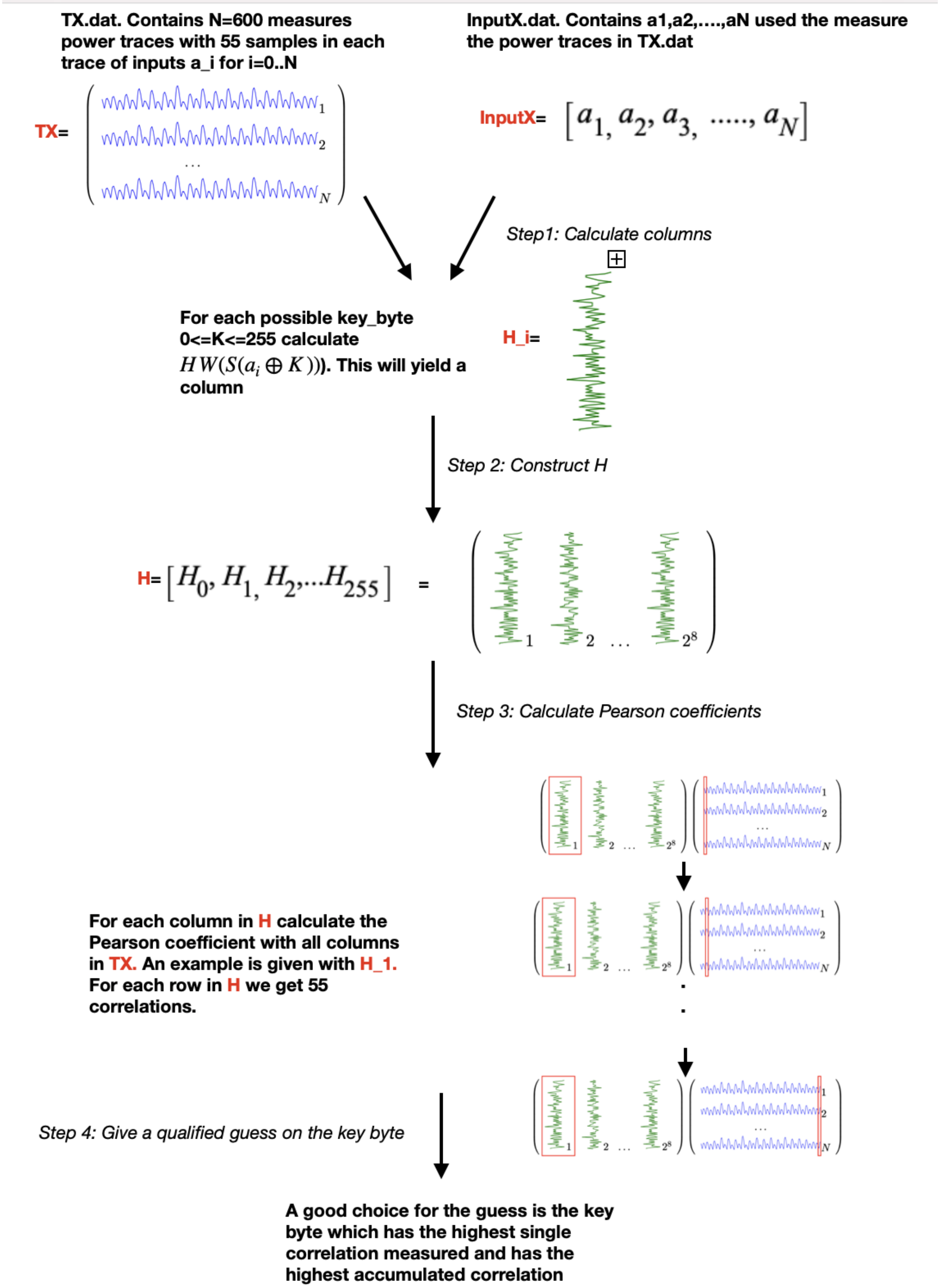
- InputX.dat: This file contains N=600 values $0 \leq a_i \leq$ for $i = 1..N$. The X in the filename is replaced by the last digit of our student numbers - 6 and 3 respectively.
- TX.dat: This file contains the power trace with 55 samples of the N values in the InputX.dat file

Now we assume that the power consumption of the device measured is proportional to the hamming weight of the input a_i (or more specifically the encrypted version of the input) for $i = 1..N$. The attack now proceeds as follows

- First we choose a possible value K of the key-byte we want to guess.
- For each a_i in InputX.dat we calculate $HW(S(a_i \oplus K))$ (where HW is the hamming weight and S is the AES S-box) and save this as a column in a matrix H.
- This is repeated for each possible value of the K (0-255). There are 2^8 such values so H is a 600×256 matrix.
- Now we do not know when the encryption happens on the device we are attacking but we know that the hamming weight is proportional to the power consumption. Hence we calculate the pearson correlation of a column in H with each possible time point (which there are 55 of) in the power trace (each column in TX.dat)

- For each guess of the key-byte we will get 55 correlations since there are 55 samples. We then both look at the accumulated correlation for each key byte and the single maximum correlation found (which means the correlation closest to 1 or -1).
- Now if the guess of the key-byte is wrong the probability that we will get a good correlation (whether is the max or the accumulated) is low. Hence our guess of the key byte will be the key byte where the maximum correlation occurs (or the maximum accumulated correlation occurs).

The attack is illustrated in the following figure:



TX.dat. Contains N=600 measures power traces with 55 samples in each trace of inputs a_i for i=0..N

InputX.dat. Contains a1,a2,….,aN used the measure the power traces in TX.dat

TX=
1
2
…
N
InputX= $[a_1, a_2, a_3, \ldots.., a_N]$
Step1: Calculate columns
H_i=
Step 2: Construct H
H= $[H_0, H_1, H_2, \ldots H_{255}]$ =
1
2
…
2^8
Step 3: Calculate Pearson coefficients
Step 4: Give a qualified guess on the key byte

For each possible key_byte 0<=K<=255 calculate $HW(S(a_i \oplus K))$). This will yield a column

For each column in H calculate the Pearson coefficient with all columns in TX. An example is given with H_1. For each row in H we get 55 correlations.

A good choice for the guess is the key byte which has the highest single correlation measured and has the highest accumulated correlation

Figure 1: Illustration of DPA attack with a hamming weight model performed on AES

3 Result for T3.dat and Input3.dat

When running the attack on T3.dat and Input3.dat we got the following result

- Our guess of the key-byte is $0x20$ (32 in decimal)
- This key-byte had the maximum correlation coefficient equal to 0.317993
- This key-byte also had the highest accumulated correlation coefficient of 9.300139
- For comparison the second highest accumulated correlation coefficient was 7.655247 (for key 186) and the next highest correlation coefficient was 0.188788 (for key 223)

4 Result for T6.dat and Input6.dat

When running the attack on T6.dat and Input6.dat we got the following result

- Our guess of the key-byte is $0x18$ (24 in decimal)
- This key-byte had the maximum correlation coefficient equal to 0.331466
- This key-byte also had the highest accumulated correlation coefficient of 9.162978
- For comparison the second highest accumulated correlation coefficient was 7.761206 (for key 140) and the next highest correlation coefficient was 0.186642 (for key 56)

5 Conclusion

By using both the maximum correlation and the maximum accumulated correlation our DPA attack on AES yielded the following results:

- For T3.dat and Input3.dat the key byte is 0x20 (32)
- For T6.dat and Input6.dat the key byte is 0x18 (24)

Furthermore we can see that the next best key guesses based on the maximum correlation or the maximum accumulated correlation seems to be must lower than our key guesses which makes the probability that our key guesses are correct higher. We can also see that it is not the same key-byte which has the next highest maximum correlation and maximum accumulated correlation, which again could point to the direction that our guesses of the key-bytes are correct.