Lab 3 - Correlation Power Analysis Attack

Due on Feb. 12 (T), 2019

1 Description

In this lab, you will implement a correlation power analysis (CPA) attack and recover all 128-bit AES key used in the last round operations. You will need to download a set of power traces of 128-bit AES running on an FPGA board. You will first examine the power traces and understand the implementation and the suitable power model. You are told which time point is the most leaky one, and you will need to utilize this leakage point to perform the correlation power analysis and recover the key.

2 Data Set

Go to `http://tescase.coe.neu.edu/?current_page=power_trace_form&software_id=0&trace_type=ptunmasked` and download a set of 50,000 unmasked power traces. Under the **Request Information**, select *AES* for **Data Type**, *Unmasked* for **Mask**, and *50000* for **Number of Traces**. Fill out rest of the form and submit the form. After you submit the form, it will send you a shell file to your email. Use the shell file to download the data.

Once you unzip the downloaded data, you will see the following files:

1. 001_cipher.txt
2. 001_corr_int.fig
3. 001_corr_int.png
4. 001_plain.txt
5. 001_trace_int.txt

You will need to use *001_cipher.txt* and *001_trace_int.txt* for this lab. Each row of both files is for one encryption, which consists of one 16-bytes ciphertext and one 3125-point power trace, respectively.

Use any programming language you are familiar with, such as Matlab and Python. First, you will need to generate a plot of one power trace in the data set. You should see 11 dips in your plot. **Explain why there are 11 dips instead of 10 dips**.

Organization of AES State: The state of AES is organized as in Table 1. Its index is increasing along the rows.

0	4	8	12
1	5	9	13
2	6	10	14
3	7	11	15

Table 1: AES 16-Byte State

3 Correlation Power Analysis with Hamming Distance Power Model

For this part of the lab, you will need to use the Hamming Distance (HD) power model to recover all 16 AES key bytes. With the correct key byte value, the HD model has the strongest correlation with power traces at time point 2669 (HD Leakage Point). Recall that each cipher byte is computed as $c_i = sbox[s_j] \oplus k_j$, so the HD model will be $HD(c_i, s_j)$ or $HD(c_i, inv\_sbox[c_j \oplus k_j])$. With each key byte guess, using this HD model to correlation with power traces at the leakage point. The correct key byte value should be the one with the strongest correlation. Note: You will need to consider the ShiftRow operation when you are performing the HD analysis. Refer to Table 1 when computing ShiftRow.

4 What You Need to Turn In

To receive credit on this lab, you will need to turn in all your code, and following items:

1. A plot of one power trace
2. A plot showing all key bytes recovery using HD model
3. Recovered last round AES key bytes

```
$ zip [your last name]-lab3.zip codes key.txt powerplot.pdf hdkeyrecovery.pdf
```

5 Extra Credit

Bonus point:

1. *Attack Without Knowing the Leakage Point (10 points):* You are given the leakage point when you are performing the attack. In reality, an adversary would not know the leakage point. However, he can have an educated guess of the range of time points where the last round of the AES encryption happens, e.g, in the range of [2600, 2800]. CPA based on HD power model has to be performed on all the time points, as explained in class. You will obtain a 2-dimensional matrix of Pearson correlation coefficients (both time dimension and key-space dimension). The highest value in the matrix will give out both the corret key bute value and the most leaky point. Verify if the leaky point you find is indeed point 2669.
2. *Attack Using Hamming Weight (HW) Power Model (20 points):* For this extra credit, you will need to first identify the leakage point due to the Hamming Weight model of the last round state ($HW(s_j)$ or $HW(inv\_sbox[c_j \oplus k_j])$) and perform an attack using the hamming weight power model. Since you have already recovered the correct key byte value. Use the last key byte value (k_{15}), compute the last round state, and perform the HW analysis for each time point in the range [2600, 2800]. Use the time point with the strongest correlation value as the HW leakage point. Now, use the HW leakage point and perform HW analysis to recover all key bytes. **Can you recover the key byte using the HW model? If not, please provide your reasoning.**