CS6630 Assignment 2: Power Analysis

Saurav Kale (EE19B141), Arun Krishna AMS (EE19B001)

September 1, 2022

1 Answers to Q1, 2, 3

Q1.

```
RK0[0] =  204   Correlation =  0.020107257378350854
RK0[1] =  74   Correlation =  0.03802331665636959
RK0[2] =  210   Correlation =  0.019211783625898315
RK0[3] =  201   Correlation =  0.02301902158701511


RK1[0] =  214   Correlation =  0.01795111117181251
RK1[1] =  77   Correlation =  0.03673988864219572
RK1[2] =  173   Correlation =  0.016946847974170155
RK1[3] =  129   Correlation =  0.022773730622040265
```

Q2.

```
RK34[0] =  86   Correlation =  0.02013007047256377
RK34[1] =  74   Correlation =  0.03755618624726031
RK34[2] =  117   Correlation =  0.019865101793603376
RK34[3] =  124   Correlation =  0.023648870711137148


RK35[0] =  49   Correlation =  0.01764125784884731
RK35[1] =  183   Correlation =  0.0373867466237373
RK35[2] =  107   Correlation =  0.016725249134811722
RK35[3] =  32   Correlation =  0.022915595280868298
```

Q3.

```
RK2[0] ^ WK0 =  251   Correlation =  0.020168991765706495
RK2[1] ^ WK0 =  229   Correlation =  0.037872538222037316
RK2[2] ^ WK0 =  57   Correlation =  0.01894024655195344
RK2[3] ^ WK0 =  54   Correlation =  0.02346715715564402

RK3[0] ^ WK1 =  246   Correlation =  0.017784731239705132
RK3[1] ^ WK1 =  3   Correlation =  0.03683092280212378
RK3[2] ^ WK1 =  132   Correlation =  0.01682824386803283
RK3[3] ^ WK1 =  149   Correlation =  0.023415981096627774
```

2 Report: CPA on CLEFIA-128

Correlation Power Analysis was carried out on our implementation of CLEFIA-128

2.1 Method of attack

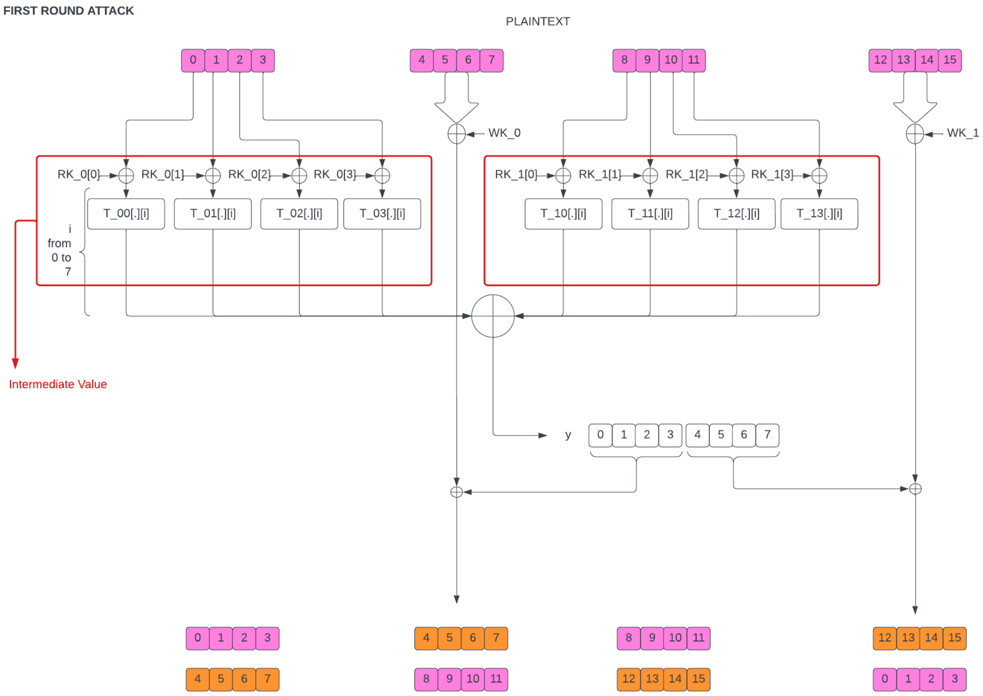


Figure 1: Block diagram of the first round attack on CLEFIA-128

Figure 1 illustrates both the structure of our t-table implementation for CLEFIA-128, as well as the intermediate value we chose for our CPA on round 1.

- We choose to attack the bytes 0 to 3 and bytes 8 to 11 of the plaintext because they are not polluted by adding the whitening keys. This is our observable. This will help us extract the round keys RK_0 and RK_1 used in the combined fiestel structure we have implemented in the form of t-tables.

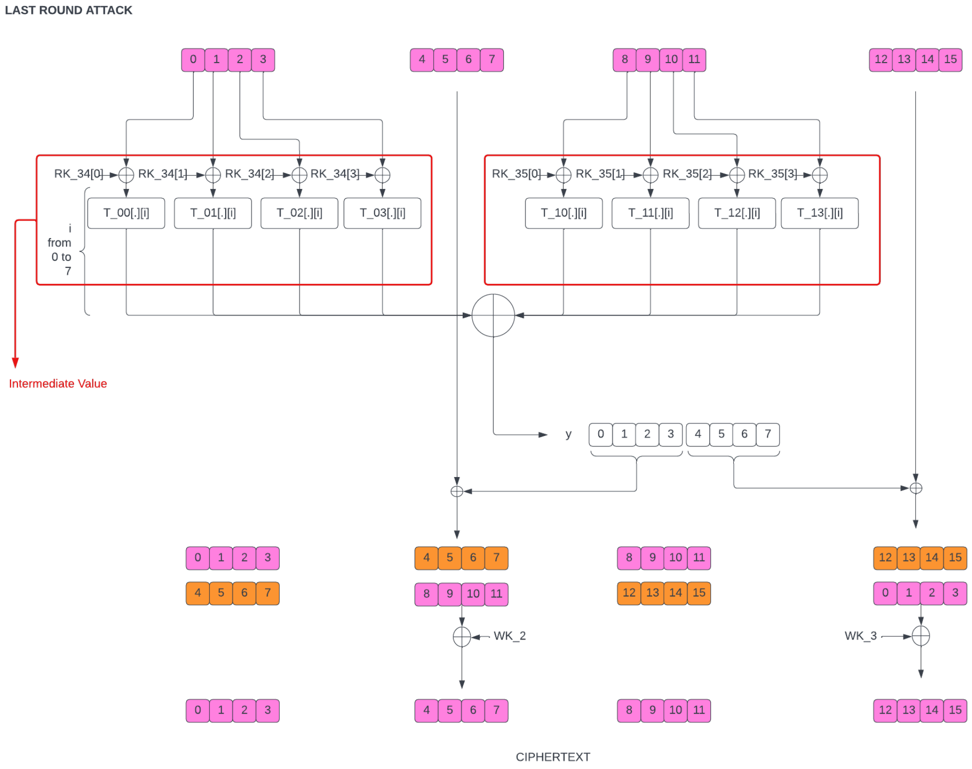
- For our power model, we have chosen the Hamming Wieght model.

- The reference code was targeted towards AES, which has all the 16 bytes of plaintext add to the round key, and then go through the same s-box in round 1. However, for CLEFIA, we need to attack two 4 byte parts of the 16 byte plaintext. Also, the fiestel structure has two distinct functions F0 and F1, which means, overall, we have to run 8 correlations in order to extract both the round keys.

- We also have to calculate the hamming wieght of the intermediate, which we do by calculating the intermediate manually (in the python code itself) and then taking its hamming wieght. This has 8 functions, each to calculate the hamming weight of the intermediate associated with each of the 8 t-tables.

- We then proceed to run the 8 correlations, each on different parts of the power trace. The start_point and end_point of each correlation is chosen approximately after taking a look at the traces. As long as the correlating part is in the interval, we are good to go, because only that part should show a high correlation with the hamming wieght calculated.

As for last round keys, we followed a very similar approach for the last round, only this time our observable was the bytes 0 to 3 and 8 to 11 of the ciphertext.



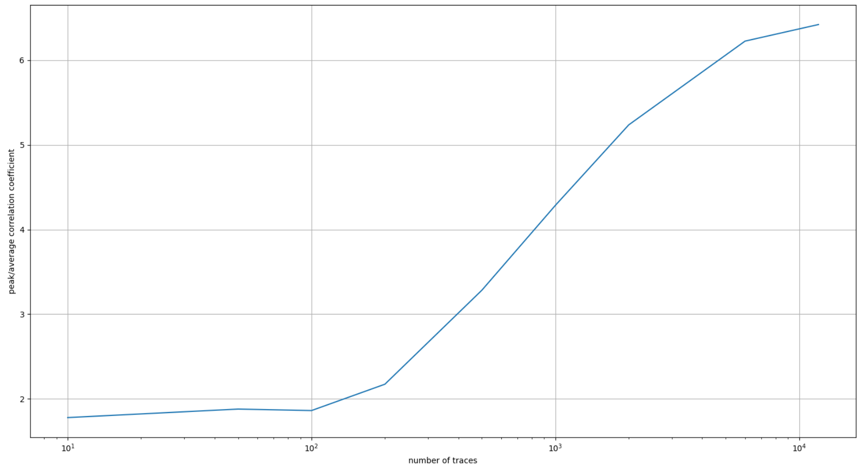
e

Figure 2: Block diagram for last round attack on CLEFIA-128

For Q3, we can target the second round of CLEFIA, since our intermediate now corresponds to key $RK_2 \oplus WK_0$ and $RK_3 \oplus WK_1$. Targeting the second round in the same way will yield these values.

2.2 Confidence in key vs. number of traces

The number of traces included in the analysis was varied from 10 to 12,000 and the peak and average correlation coefficients were obtained. Plotted below are the peak/average values of the correlation coefficient vs the number of traces.



t

Figure 3: Peak/Average Correlation coefficient vs number of traces

The peak/average increases, and then flattens beyond 6000 traces. We need a minimum of around 100 traces to get a good estimate of the key. Below 100, the values estimated have high probability of being incorrect. This is expected, since initially, there are too few traces to produce a good estimate of the key. As the number of traces increase, the correlation between the hamming wieght with correct key and power trace is much more pronounced. Adding more traces beyond a limit does not affect the correlation coefficient because the sample space is already large enough to show maximum correlation.

2.3 Why not go with Hamming distance model?

- CPA on AES encryption with Hamming Distance model would be performed between the output of Sub-Bytes operation and the output of Shift-Rows operation. In AES, the correlation would depend on just 2 keys, Thus, 256^2 guesses are required to get the two keys.
- In case of CLEFIA-128, CPA attack using Hamming Distance model would have to be performed in the input-output of word-rotation in GFN4 operation. In such an attack, the correlation would depend on 4 keys. Thus, 256^4 guesses are required to get the four keys.
- This rapidly increases the offline phase. We observed that in Hamming Weight model, a minimum of 100 traces are required. Since this is sufficiently low, we chose the hamming weight model.