Assignment 4

In week 6 lecture, we have seen how the SNR values can be computed using the *Random dataset* when the signal is taken to be the exact value of the 0th Sbox output. The POI, which is the time sample with the highest SNR, is given by 392.

The task of this assignment is to find the POI when the signal is the exact value of different Sbox outputs.

- For each $i = 1, 2, \ldots, 15$
- Take the signal to be the exact value of the ith Sbox output in the first round of PRESENT
- Compute the SNR values for each time sample using the *Random dataset*
- Take the time sample that achieves the highest SNR value to be the POI
- **Note**: for the 8th nibble, the POI should be given by the time sample that achieves the third highest SNR value

More information about the ***Random dataset***

- The dataset can be downloaded from: `https://github.com/XIAOLUHOU/SCA-measurements-and-analysis----Experimental-results-for-textbook/tree/main/random_dataset`
- There are in total $10,000$ traces
- The ith trace is stored in a file called trace_i.txt, for $i = 0, 1, \ldots, 9999$
- The ith line in the file keys.txt contains the round key used for the collection of the ith trace
  - For example, the round key used for the collection of the 0th trace is given by

    `65d9aad55c6c6ce7`,

    where the 0th nibble is `7`, the 1st nibble is `e`.
- The ith line in the file plaintexts.txt contains the plaintext used for the collection of the ith trace
  - For example, the plaintext used for the collection of the 0th trace is given by

    `e8ed1e14087c1414`,

    where the 0th nibble is `4`, the 1st nibble is `1`.

Question 1. (3 marks – 0.2 marks for each POI) Write down all the 15 POIs you have found

Question 2. (1 mark) Plot the SNR values corresponding to the signal being the exact value of the 3rd Sbox output.

Note: Half of the grade will be determined by the quality of the implementation details discussed during the individual meetings.

What to submit.

- The submission in AIS should include a PDF document containing responses to the aforementioned questions, along with the code utilized to complete this assignment.
- Add full name in both the file name and inside the file

When to submit: by Week 8 Thursday 8 am