Assignment 5

The objective of this assignment is to perform template-based DPA on the provided traces to recover the first-round key for the PRESENT implementation.

- In Assignment 4, Part A, POI values for each S-box output were obtained, each corresponding to a first-round key nibble, taking the target signal to be the exact S-box output values.
- Detailed profiling and attack procedures can be found in the week 8 lecture slides and in textbook Section 4.3.2.
- Use the *Random dataset* as the profiling traces and "attack_traces" from the link below as the attack traces.
- Individual meetings will be scheduled to present the implementation of the entire attack process.

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`.

More information about the "attack_traces"

- The dataset can be downloaded from: `https://github.com/XIAOLUHOU/SCA-measurements-and-analysis----Experimental-results-for-textbook/tree/main/Assignment_materials/attack_traces`
- There are in total 100 traces
- The ith trace is stored in a file called trace_i.txt, for $i = 0, 1, \ldots, 99$

- 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

    `deadbeef01234567`,

    where the 0th nibble is `7`, the 1st nibble is `6`.

Question 1. (1 mark) In your attack to recover the 2nd nibble of the round key, what template did you obtain for the target intermediate value equal to `C`?

Question 2. (5 marks) Let

$$K = k_{79}k_{78}\dots k_0$$

denote the master key. We know that

$$k_{15}k_{14}\dots k_0 = \texttt{CBAF}$$

Suppose we also know that for the plaintext

`0000000000000000`

the corresponding ciphertext is

`D0A5AEAE5F4BC249`

What is the full master key?

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 9 Thursday 8 am