Assignment Homework 3

Due date: March 1, 2023 (AoE) = Anywhere on Earth

Please complete this assignment (200 pts total) and submit your report/program code on Canvas (all files compressed in one `.zip` without the `.npy` files)

1. For this task, we consider two types of devices. *i*) device of type A implements the AES with just a single S-Box in hardware; *ii*) device of type B implements the AES with 16 S-Boxes to do a full AES round within just one clock cycle. Both devices are now studied as part of a power analysis attack. Let us consider the behavior of the noise in more detail: (20 pts)
   a) In terms of a power analysis, which device is more likely to show higher (algorithmic) noise when assuming randomly distributed plaintext inputs? (3 pts)
   b) Assuming all other device characteristics are the same, which one will be more difficult to attack? Note that difficulty of attack is the number of traces required for a successful key extraction. (7 pts)
   c) Assuming there are no algorithmic countermeasures, is it possible to adapt the attack on device of type B such that when attacking the first round of AES, the attack would behave similar to device of type A? (*hint*: the attacker only controls the plaintext input) (10 pts)

2. In previous assignments, you worked with simulated data that may not necessarily reflect reality. For this task, you will work with actual measurement data of an 8 bit microcontroller running a software implementation of the AES. This will be our first attack on actual measurement data. For this task, use the traces intended for attack, i.e., random plaintext and unknown fixed key. (30 pts)
   a) Create the SNR plot based on the plaintext input to quickly narrow down the number of points you have to work on. (10 pts)
   b) Create a plot where multiple traces with the same input data are averaged to remove the noise. Annotate the plot with at least: points in time where KeyAdd and SubBytes of the first round are performed. Identify the whole AES round. (5 pts)
   c) Run a CPA to recover the key. Try different power models such as Hamming Distance/Weight, on different intermediate values such as KeyAdd and SubBytes. What do you observe? What works best and why? (15 pts)

3. In the following, you are tasked to implement *one* of the following methods. (150 pts)
    - **Recommended for all students:** Standard Welch's t-test (1st order) [*]
        - Implement the leakage test and plot the result
        - Does the implementation show leakage? If so, where?
    - **Alternatively: additional bonus of 50 pts (total of 200 pts for this task):**
        - (Profiled) Stochastic Approach[†]
        - (Non-profiled) Linear Regression Analysis [‡]
        - (Non-profiled)/(profiled) Mutual Information Analysis or Mutual Information Metric [§]; MIA should be implemented using histograms for PDF estimation
        - (Collision) CEPACA [¶] *and* MCDPA [‖] (as they are almost identical)
        - (Leakage Detection) χ^2-test [**]

Suitable trace sets will be distributed through Box / Dropbox. Try to work on *at least* 1000 points of that trace **and benchmark your implementation**. Try determining the number of traces needed for success (i.e., create a success-metric vs. number of traces plot). Additional goals vary depending on the type of scenario:

- Profiled: create a plot showing the leakage; possibly extract key from fixed-key data set.
- Non-profiled: create a plot showing the leakage including key extraction.
- Collision: create a plot showing the leakage including key extraction.
- Leakage detection: create a plot showing the leakage.

Please write your code in your preferred programming language/environment. **Do not use any existing side-channel analysis oriented library.** Thoroughly document your code by using comments and referencing equations in the corresponding papers. Your `.zip` file should contain your code, instructions how to make it run (if needed), your report, the figures, etc.

---

[*] Welch's t-test: paper
[†] Stochastic Approach: paper 1, slides paper 1, paper 2
[‡] Linear Regression Analysis (LRA): paper
[§] MIA/MIM: Paper 1, Paper 2, Paper 3, Paper 4, Master's thesis
[¶] CEPACA: paper, Youtube video including a description of CEPACA
[‖] MCDPA: paper, paper with one-pass incremental update formulas
[**] χ^2-test: paper, video, and slides; note the appendix of the paper