Assignment 3

Due date: February 14, 2022

Please complete this assignment (200 pts total) and submit your report/program code (all files compressed in one `.zip` to `vincent.immler@oregonstate.edu` with subject as follows:

Subject: CS/ECE599 Assignment 3, Winter 2022, *Your Name*

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 noise when assuming randomly distributed plaintext inputs? (2 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. (3 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. (5 pts)
   b) For the point with the highest SNR, create a histogram plot of each different hamming weight (all in one plot). (5 pts)
   c) 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)
   d) 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)
    - (Profiled) Stochastic Approach[*]
    - (Non-profiled) Linear Regression Analysis [†]
    - (Non-profiled)/(profiled) Mutual Information Analysis or Mutual Information Metric [‡]
    - (Collision) CEPACA [§] *and* MCDPA [¶] (as they are almost identical)
    - (Leakage Detection) t-test *and* χ^2-test (since substantially less work on their own)
        - Welch's t-test [‖]
        - χ^2-test [**]
    - (Profiled/Non-profiled) SCATTER [††]

Suitable trace sets will be distributed on Microsoft Teams. Try to work on at least 1000 points of that trace and benchmark your implementation. Try determining the number of traces needed for succes. 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 all your programs in one of the following languages/environments: Python/Jupyter. Thoroughly document your code by using comments and referencing equations in the papers. Your `.zip` file should contain your code, instructions how to make it run (if needed), the figures, etc.

---

[*] 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
[‖] Welch's t-test: paper
[**] χ^2-test: paper, video, and slides; note the appendix of the paper
[††] SCATTER attack: paper, reference in Matlab