CS529-HWS: Hardware Security - Lab 3

Dave (Jing) Tian

April 28, 2025

1 Deadline

By the end of May 7th, 2025 (EDT)

2 Goal

Applying differential power analysis (DPA) on a tiny AES implementation using ChipWhisperer Nano

3 Description

This lab reuses the "Lab 3-3 DPA on Firmware Implementation of AES" from ChipWhisperer-Jupyter courses, e.g., `chipwhiperer-jupytercourses/sca101/Lab 3_3 - DPA on Firmware Implementation of AES (MAIN).ipynb`. Make sure you can connect your ChipWhisperer Nano and collect power traces accordingly. Moving forward, you will realize that the DPA attack essentially chooses **bit-0** as the rule/policy to partition power traces. But,

- What about using other bits in the output as the rule to partition power traces, e.g., **bit-X**?
- For the recovery of each subkey (byte, or round key), what would be the best **bit-X**, e.g., yielding the most significant differences compared to other guesses?
- Does it exist the best **bit-X** that is simply the best for each subkey recovery?

- If **bit-0** is not the best global partition policy, how would you choose your partition policy?
- Explore all the questions above with the number of traces in 1K, 2K, 2.5K (default), and 5K.

4 Deliverable

Answer the questions above using the Python code and plots you will add to the Jupyter notebook. Note that this lab does **not** require the solution for the original lab 3-3, but your answers with supporting evidence to the questions above. As usual, please put your code and data into a PDF report (or just convert your notebook to PDF if it is easier). At the end of your report, please write a short paragraph regarding the takeaway based on your answers.

5 Grading

20% penalty for each day of delay after the deadline. If any two reports look similar to each other (judged by the professional cheating software), both reports will receive zero credit. They will be reported to the grad school for further investigation.

6 Others

This lab assignment does not allow for teaming. You should finish this by yourself. Given the detailed instructions from the notebook, discussion with peers is not allowed.

7 Warning

Please be cautious about ESD. Try to ground yourself and/or the working bench before you start to poke around the device. Assuming you have a laptop/desktop connected to the power cable, you can touch the metal part of the case for ESD as the bare minimum protection.