TTM4205: ChipWhisperer Lab Fall 2024

Tjerand Silde and Caroline Sandsbråten

{tjerand.silde, caroline.sandsbraten}@ntnu.no

Assignment

This is one out of three assignments in the course TTM4205 Secure Cryptographic Implementations (ttm4205.iik.ntnu.no) during fall semester of 2024.

This assignment has to be solved *individually*, except for Section 4 (Bonus Problem: RSA Lab), as we do not have enough XMEGA target boards. Then you are allowed to work in pairs. The solutions and answers to the tasks must be *your own*. It is, however, *allowed* to discuss the problems with other students and ask for hints or pointers from the course staff.

It is *allowed* to rely on external resources to solve the lab assignment; however, these resources must be *clearly* referred to. Otherwise, it will be considered cheating; see i.ntnu.no/wiki/-/wiki/English/Cheating+on+exams.

The ChipWhisperer lab assignment contains problems related to side-channel and fault attacks. The problems are adjustments of the problems available at github.com/newaetech/chipwhisperer-jupyter.

All problems require detailed answers where you describe and document what you have done to complete the task, e.g., written explanations, calculations, code, graphs, etc.

All submissions must be written in LaTeX, and we provide a mandatory template to be used at overleaf.com/read/mrpwqqxdkbfv#667c9c.

The assignment and the installation guidelines are available as a zip-file at the course wiki at github.com/tjesi/TTM4205/blob/main/CW/2024/CW.zip.

This assignment counts for at most 20 points, and each topic is marked with how many points it is worth, roughly estimating how much work is expected. The bonus problems are not expected to be solved but can give up to 5 additional points each to make up for missed points elsewhere. We also give full or partial credit if you show that you understand a problem and made an attempt to solve it even if you are not able to solve it entirely.

Submission deadline: December 6th at 23:59 in Ovsys2.