Reference group meeting TTM4205 on 09-12-2024

Attendees: Tjerand, Caroline, Emil, Jiaqi, Daniel

Topics we discussed:

- *Lectures*
  - Students appreciated the guest lectures since they explained well and gave insight into relevant topics not covered by the curriculum in the course
  - Lectures and discussions where helpful to get an overview of the different topics and to understand the foundations covered in the course, and the slides and referenced resources were helpful to get started solving exercises and conducting lab assignments
  - Topics that could be covered in more detail in the start of the semester:
    - IND-CPA, IND-CCA, CRT, ECC, Finite Fields, and similar
    - We should detail background knowledge more in first lecture
- *Exercise class / lab*
  - The CW setup lecture was very helpful to get everything working and get started with the assignments, it should be given twice next year
  - It was also useful to collaborate with other students on the lab
  - We should make the software available on more machines outside of the lab
- *Assignments*
  - There is a lot to do in this course, and there are many difficult tasks to solve. But on the other hand, it is not unreasonable regarding the course not having an exam at the end, and the students gain a lot of knowledge working on it.
  - Some weekly problems are quite mathy, so it might require some more background or explanations in the lectures or exercise sheet next year.
  - The ChipWhisperer exercises should give more context for the tasks and what is happening, in addition to the shorter descriptions about what to do.
  - The timeline for the technical essay is working out well, and the presentations were insightful and encouraged the groups to get started.
  - The distribution of points for the three projects is reasonable, but we should emphasize (even) more that it is a lot to do, that students should start early working on the exercises and lab assignments and go to exercise classes.
- *Ed Forum*
  - It is a good resource and way to get help and should be continued next year.