Reference group meeting 23/11-23

Attendees: Tjerand, Espen, Diderik, Nimer, Simen, Jonathan

Topics that we discussed at the meeting:

- Lectures
    - A lot of interaction was a great incentive for attending lectures
    - Really cool and relevant guest lectures, could be announced more broadly next year (only Vadim's talk was announced this time)
    - Continue referring to chapters, blog posts, papers etc to read up
    - Continue keeping the content updated by including recent works

- Exercises class/lab
    - Do the first CW exercise with everyone in the exercise class
    - Might need two TAs next year in case more students sign up

- Exercises
    - Extend the deadline to midnight December 10th? Yes.
    - Make the RSA fault injecting a bonus problem?
    - Have two deadlines for exercises instead of one
    - The first two CH exercises are the hardest ones
    - How to make Sage work on all machines: CoCalc (notebook)
    - Give a tutorial on the crypto library used for CryptoHack
    - Unplug CW between labs (disconnecting doesn't work well)
    - Remark when to use nano vs level 1 kit for CW exercises
    - Promote the Discord for the CryptoHack problems
    - Adjust the ECDSA lecture to be more aligned with the CH problem