

Final project instructions

You can choose to do a final project or sit for a final exam.

The final research project is an opportunity for you to independently explore some topic. You can do this alone or with a partner. Any topic relates to programmable cryptography or secure secure computation will work: applied or theoretical topics are both fine.

Think of the goal for the project as being a (weaker) tutorial paper, workshop paper, or research poster. Something that is **not** (yet) publishable research, but could be the starting point for a research project.

If you are already working on some external research project related to programmable cryptography and you want some part of that project to count for this course, that is okay and is even encouraged.

Examples include:

- You read a some research papers on class of programmable cryptosystems and write a survey paper/tutorial about that class of cryptosystems.
 - These systems might be applied (focused on concrete efficiency or particular applications) or theoretical.
 - Examples: distributed point functions, functional encryption, private function evaluation, maliciously secure MPC, sumcheck-based ZKPs, compressed sigma protocols, oblivious RAM, ...
- You design and implement a privacy-preserving computer system using programmable cryptography.
 - privacy-preserving trajectory estimation for AirTags?
 - a privacy-preserving loyalty program?
- You study an interesting societal dynamic, formally define security for it, and show how some cryptography-based system can be used to provably achieve that security.

Proposal

You must submit your project proposal at 6pm, Friday October 23rd. You may not use late days.

The proposal must:

- be 1-2 pages
- give a quick description of your topic
- clearly explain what you plan to do, for example:
 - which papers you will read
 - what software you will design and implement
 - what informal notion of security and privacy you will formalize

Your final project needs to have the right level of difficulty and interestingness. The proposal will help us get that right: I'll give you feedback on your proposal so that you can adjust your plans for the project.

Project deliverables

- The **proposal** (1-2 pages, due date: Oct 23)
- A written **report** (5-10 pages, due date: Dec 7)
- If the project has **software**, a zip file. (due date: Dec 7)
 - Instructions for running the software should be in the report.
- A **presentation** (15-45 minutes, due date: Nov 30 – Dec 7)
 - We will have three class days for project presentations. The exact presentation length will be announced once we know how many projects there are.
- An **oral exam** (20 minutes, time: TBD)

Grading

The project is 25% of your grade. Here is the breakdown in criteria:

- **Proposal** (1%)
 - This will be graded for clarity: how clear is your topic description, plan, and what you think you will accomplish.
 - It **is** important that your project has the correct level of difficulty/interestingness. But, your *proposal* grade does not depend on that. If the project is too easy or hard, I'll let you know in my feedback so that you can adjust your plans.
- **Presentation** (10%)
 - The target audience is the class (not me).
 - This will be graded on how well you motivate your problem, how engaging you are, and clarity.
 - During presentations, **attendance is mandatory**. Part of your grade is attending and asking questions after others' presentations.
- **Report/software** (14%)
 - The target audience is me.
 - These will be graded for clarity, correctness, and interestingness.
 - If your proposal is good and you end up following it, then that probably gets full marks for "interestingness".
 - Deviating from the plan is good too, if you find a more interesting path.
- **Oral exam**
 - I will ask you technical questions about your talk, report, and software.
 - There will be a whiteboard and you may need to explain some things.
 - There will be a sign-up sheet for scheduling this.
 - This is a check against using too much AI. It isn't worth any points, but if it seems that you do not understand your project, you will lose points from other categories.

Pairs

If you work in a pair, the standards are higher, but not 2x higher. You will submit all deliverables as a team on Gradescope. You will also present together, and should split the time roughly evenly. You'll also do the oral exam together.