Math 480A2 Final Project

During the last month of the semester, you will have the opportunity to explore a topic of your choosing related to the material from the course. You will take some time to familiarize yourself with a topic of interest, write up an overview of what you've learned, and give a short presentation summarizing the topic to your classmates. The grade for your project will contribute 20% to your overall course grade. Half of the project grade will be based on your write-up, and the other half will be based on the presentation. The project may be completed individually or with a partner.

Write-up

The write-up should aim to introduce and summarize your topic to somebody who has a good working knowledge of the material we've covered in the course, but who may not know the specifics of the particular topic you are covering. You should give an overview of what your topic is about, what it does or accomplishes, and how it relates to what we've covered in the course. Describe any important definitions, algorithms, and main theoretical results, and include diagrams and examples as appropriate. You may want to include one or more short proofs for results that are not too complicated, but feel free to just give the statements of results whose proofs are long or technical. The goal of the write-up should be to present a practical view of what your topic is about, and what it is useful for. Your submission should be 3–6 pages typed (using LaTeX is encouraged for this purpose, but not required), and should include a short bibliography of your main references for the material.

Write-up Rubric:

- Submission is 3–6 pages, typed
- Submission describes the chosen topic in enough detail that the purpose and workings are clear
- Submission provides the main definitions, algorithms, and theoretical results relevant to the chosen topic
- Submission explains applications of the chosen topic, and how it relates to material covered in the course
- Technical content in the submission is correct, e.g. definitions, algorithms, theorems, and proofs
- Submission is proofread for correct spelling and grammar
- Submission includes a short bibliography with the most important references used

Presentation

The presentation should aim to teach the class about what you learned! Summarize the material in your write-up, explain any important algorithms or protocols, work through examples, and describe applications and use-cases. The format for the presentation can be flexible; your presentation can use slides on a laptop or be written out on the board, and you can feel free to demonstrate the usage of software related to your topic if applicable.

Presentation Rubric:

- Presentation is 10–20 minutes
- Presentation summarizes and explains the purpose of the chosen topic
- Presentation provides the main definitions, algorithms, and theoretical results relevant to the chosen topic
- Presentation is clear and informative, and is framed appropriately to be understandable by the classroom audience

Topic Ideas

The following is a non-comprehensive list of possible topics for the final project. If there is a different topic that you would like to explore instead, please check with the instructor to confirm that the topic is a good fit for the goals of the project. Section and chapter references below are in *Proofs, Arguments, and Zero-Knowledge*, by Justin Thaler.

- Algorithms for computing discrete logarithms
- A super-efficient interactive proof protocol for matrix multiplication (§4.4 and §4.5)
- GKR circuit evaluation protocol (§4.6)
- Commit-and-prove argument from Pedersen commitments (§12.3, §13.1, and §13.2)
- Bulletproof polynomial commitment scheme (§14.4)
- Arithmetization techniques (Ch. 6)
- Multiparty Interactive Proofs and Probabilistically Checkable Proofs (§8.1 and §9.1)
- Merkle, Merkle-Patricia, and Verkle trees (§7.3.2.2 and elsewhere)
- FRI protocol (§10.4)
- SNARK composition and recursion (Ch. 18)