CS/ECE407 – 4 Credit Hour Project

Due: Wednesday, May 6, 11:59pm CT

Summary

As a student enrolled in the four-hour version of the course, you are expected to go above and beyond the standard cryptography discussed in lecture. The goal of this project is two-fold:

- Take a deep dive on a particular topic and learn its advanced techniques.
- Learn about the research side of cryptography more generally. For example, learn how papers tend to organized, how to find papers relevant to your question, etc.

You and up to two teammates will select an advanced topic in cryptography, read research papers on your chosen topic, and write a literature review. Your objective is to present a coherent explanation of an advanced topic in cryptography. In particular, your review should:

- Explain the **context** of your chosen topic. Why do cryptographers care about your topic? Why do practitioners care about your topic? How does your topic relate to the basics of cryptography? Are there any applications today? Could there be applications in the future?
- Describe the **history** of your chosen topic. What were the major advances in your topic? What is the current status of your topic? Do there remain unsolved problems? Are there trade-offs between different advances?
- Sketch **technical ideas** underlying your topic. Choose a small number of constructions/proofs related to your topic, and sketch how they work. Here, we are expecting *clear discussion* focused on main ideas. We do not expect to see huge amounts of detailed-oriented formal specifications. You are demonstrating that you understand the topic well, not that you can copy/paste the content of a paper.

View the audience to your review as an individual who has *heard* of your topic, but does not know the details. They want to read your review to understand the landscape of the topic and find pointers on where to look next.

Requirements

- You must discuss your topic with me! Come to office hours, or contact me by email, and suggest topics you might be interested in. You should contact me by **March 13**. When you speak with me, have your teammates selected and *at a minimum* have preferences on topics. The goal of meeting is to fix a particular topic and increase the chances you will succeed. As you work on your project, feel free to consult with me.
- Write your review in LaTeX. Your review should be at least **10 pages** long (in `\documentclass{article}` format, not including citations). Feel free to write as much as you want, but if you need more than 18 pages, separate your review into a main text (at most 18 pages) and appendices (unlimited length).
- Use `\section`, `\subsection`, `\paragraph` environments to clearly organize your paper, and use tables/figures/code/diagrams/theorems/etc. as needed. Again, the emphasis of this project is to *clearly explain* an advanced cryptographic topic.

- You are expected to focus on a minimum of **three** papers from the literature. However, there is no limit on the number of focused works. The appropriate number of papers will depend on your topic. You must cite more than your focus papers. At minimum, cite **eight** *published* works from competitive research venues (see list of conferences at the end of this document for examples). Here, the citations of your chosen works, as well as Google Scholar, are your friends; follow a trail of papers, and you can easily find dozens of relevant works. Outside these eight, feel free to cite anything you feel is appropriate: blog posts, videos, etc., are all fair game.
- Your review is due by midnight on the university's last day of instruction. Simply send a single email containing your review (as a pdf) to me and the course staff.

Evaluation

In evaluating your review, we will consider the following categories, each with equal weight:

- **Clarity**. The review is clear and easy to understand. The writing is free of spelling errors and (mostly) free of grammatical mistakes. The review is cohesive, and there is a clear flow of ideas that describes to the reader the chosen topic.
- **Context/History**. The review clearly describes the "what" and "why" of the topic. It explains why experts care about the problem, and how the topic has progressed. An A+ review will connect the topic to other areas of cryptography/computer science, e.g. by explaining how the chosen topic compares to other topics.
- **Mastery**. The review clearly describes the "how" of the topic. Technical details are laid out, and such details are clearly explained and free of errors. The writing demonstrates the authors clearly understand ideas in the selected topic. *Note:* there is simply *no way* you will be able to explain *all* technical ideas. Focus on ideas that seem central. We prefer clear explanation of a few ideas over bad explanations of many ideas.
- **Breadth**. The review touches on a broad selection of ideas within the topic area, and explains how they connect/compare with one another.

Potential topics

In no particular order, potential topic areas include—**but are not limited to**—the following:

- Lattice-based cryptography.
- Post-quantum cryptography (e.g., post-quantum signatures).
- Threshold cryptography (e.g., threshold signatures).
- Quantum cryptography.
- Succinct proofs (e.g. SNARKs).
- Frameworks for security definitions (e.g. Universal Composability).
- Proofs of separations between cryptographic objects (e.g., separations between public-key crypto and random oracles).
- Advanced reductions between cryptographic objects (e.g. OWFs imply signatures).
- Advanced techniques for blockchains (e.g., proof of space/proof of stake).
- Searchable Encryption.
- Secure Multiparty Computation.

- Garbled Circuits/Randomized Encodings.
- Private Set Intersection.
- Private Information Retrieval.
- Oblivious RAM.
- Fully Homomorphic Encryption.
- Functional Encryption.
- Program Obfuscation.
- Function Secret Sharing.
- Homomorphic Secret Sharing.

If you need more inspiration, have a look at the proceedings of recent cryptography research conferences:

- Crypto,
- Eurocrypt,
- TCC,
- Asiacrypt,
- Real-World Crypto.

If you need yet more inspiration, you can look for cryptography results in security-focused conferences (e.g. IEEE Security and Privacy, CCS, USENIX) or in theoretical computer science conferences (e.g. STOC, FOCS). Also applicable are works that focus on implementation of cryptography, which might arise in venues focused on programming languages, hardware design, and more.