CS 598 DH Final Project

David Heath

Abstract

For your final project, you will form a team of three individuals, choose a topic in the field of cryptographically secured computation (e.g., MPC, ZK, ORAM, etc.), select research papers related to that topic, read those papers, write a literature review, and present your topic to the class.

This document provides a rubric, as well as a template for your review. Your review should be 15–25 pages long (not including your bibliography) and typeset in a single column with 11pt font. You may use the format of this document. Note that the margins in this format are wide.

Your presentation will be 25–35 minutes long. You will discuss your topic, with an emphasis on *exposing* your peers to the key ideas of your exploration. 35 minutes is not enough time to give *all* technical idea, so focus on clearly presenting high level insights.

You are not *required* to use this template, or even to use LaTeX, though I recommend it.

1 Summary

For your final project, you will select a handful (e.g., 1–3) of academic papers as the focus of your review, and write a 15–25 page (not including citations) review on these papers. Your goals in this review are to:

- Explain the context of your chosen topic. Why do cryptographers care about your topic? How does your topic relate to topics discussed in class? 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 the main technical ideas underlying your topic. Choose a construction/proof related to your topic, and sketch how it works. Here, we are expecting to see a clear explanation, but we do not necessarily need to see a full rigorous write-up. You are demonstrating that you understand the topic well.

View your reader as a knowledgable cryptographer who may have heard of your topic, but who has not studied it in detail. Your reader wants to learn the main

ideas, and they want pointers to good follow-on materials where they can learn more.

Your review is due at midnight on **the last day of course instruction (May 1)**.

You will also present your topic. Your presentation will be 25–35 minutes long. You will **make and submit a pdf slide show**. We will have 10 groups and 2 presentations per day. We will reserve 7 presentation days, though only 5 will be used:

- April 9, April 11, April 16, April 18, April 23, April 25, April 30

1.1 Rubric

Your first task is to *form teams* and start thinking about a final topic. **Form your team and discuss your topic with me by Friday March 8 (the day before Spring break).**

Your grade will be weighted as follows:

- 65% write-up.
- 35% presentation.

Both deliverables will be graded according to the same rubric. I am looking for the following, with equal weight:

- **Context/History**. You clearly describe the "what" and "why" of the topic. You explain 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, especially those discussed in class.
- **Mastery**. You clearly describe the "how" of the topic. Technical details are laid out, and such details are clearly explained and free of errors. You clearly demonstrate that you understand ideas in the selected topic. In the presentation, you are able to answer non-trivial questions about your 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.
- **Clarity.** Your review is clear and easy to understand/You give a clear and interesting presentation. Your classmates should learn something. Your writing/slides are clear and precise. Please avoid putting "walls of text" in slides.
- **Participation/Interaction (presentation only).** When presenting, I would like to see you engage with your classmates. Consider having questions and/or discussion points prepared for the class. *When others give their talk I expect you to be present and engaged.*

The rest of this document provides some tips for organizing your review.

2 Introduction

Write an introduction that is high level, clear, and reasonably short. What is the problem? What are the existing solutions? What is your review going to talk about?

It can be useful to add labels to your sections so that you can refer to them by name. As an example, I can forward reference to Section 3.

3 Preliminaries

If necessary, include a section that covers background material required to understand your topic.

3.1 Organization

I encourage you to use sections/subsections/paragraphs to organize your document.

Equations. When writing mathematics, avoid writing math inline unless it is short and clear. For example, it is acceptable to write $x + y$ inline, but for longer expressions or equations, consider breaking out designated lines:

$$(a + b) + c = a + (b + c) \qquad \text{associativity}$$
$$a + b = (a + b) \qquad \text{commutativity}$$

4 Citations

I expect you to include professionally organized citations to peer-reviewed, reputable sources. As an example, let's cite the classic GMW paper [GMW87]. Please do use alphabetic citations.

The `CryptoBib` database provides an *excellent* collection of references to high quality cryptographic references.

It is acceptable to cite non-academic resources (e.g., blog posts, web pages, GitHub projects, etc.), but your report should focus on the academic literature. As an absolute bare minimum, make sure you cite at least five academic papers.

Where to look for citations? When searching for resources, the IACR `ePrint` archive provides a high quality collection of freely accessible papers. Most (though not all) cryptographic papers appearing at top venues are on ePrint. Not all papers on ePrint are peer reviewed.

A simple Google Scholar search can be an effective way to find related works. Start from a paper that interests you. Then, (1) look at the papers the authors cite and (2) use Google Scholar to find papers that cite them.

Which citations are reputable? If a paper appears in one of the following journals/venues, we will consider it reputable:

- Any IACR conference, especially IACR Crypto and IACR Eurocrypt.
- The Journal of Cryptology.
- Reputable security conferences, e.g. USENIX, CCS, IEEE S&P.
- Reputable conferences on the theory of computing, e.g. STOC or FOCS.

This is *far* from an exhaustive list, and resources that appear elsewhere may also be reputable. If in doubt, just ask me.

5 Collaboration

Your project is to be completed in small teams. I therefore recommend writing your report in LaTeX via `Overleaf`. Overleaf will allow you to write the paper in parallel. Just make a new project, share with your collaborators, and, if you like, you can upload this template to your project.

References

[GMW87] Oded Goldreich, Silvio Micali, and Avi Wigderson. How to play any mental game. In *Proceedings of the Nineteenth ACM Symp. on Theory of Computing, STOC*, pages 218–229. ACM New York, NY, USA, 1987.