Queen's University
School of Computing

CISC 468/870: Cryptography
Course Project Description
Fall 2022

Choosing Your Topic

CISC 870 projects are expected to be more research-focused, and CISC 468 projects may be more implementation-focused. To get started, you should frst select a general area that interests you, and then formulate a specific goal.

Selecting a general area. Examples include cracking-resistant password vaults, trusted execution environments, homomorphic encryption, zero-knowledge proofs. secure multi-party computation, cryptocurrencies, and encrypted messaging.

Formulating a goal. For **implementation-focused** projects this may be to implement a tool, system, or attack technique. You may either re-implement an existing technique from literature or you may apply a technique to solve a problem of interest to you. For example, you may apply secure multi-party computation or homomorphic encryption to solve an interesting problem. Or, you may implement and compare a number of algorithms/protocols from the same family/category (e.g., password-authenticated key exchange protocols).

For **research-focused** projects, you should compare, contrast, classify, and analyze a set of techniques or mechanisms that fall within the general area that you chose. For example, you may consider different key derivation functions, homomorphic encryption algorithms, or cryptographic algorithms used in cryptocurrencies. A research-focused project must demonstrate a **thorough** understanding of at least four academic papers, and must contain a unique contribution, e.g., by proposing a new idea or evaluating (via implementation/experimentation) an existing technique on a problem or application area of your choice.

You will need to submit a project proposal (requirements outlined below) by Oct. 24, 2022. Upon approval, you will go through the knowledge-discovery process by learning about the general area and achieving the goal that you set.

Groups

Undergraduate (CISC 468) students **may** complete their projects either individually or in groups of two (larger groups will not be permitted). If done in groups of two, each student must submit their own implementation and demonstrate that their implementations are interoperable (e.g., if one group member's implementation encrypts a message, the other should be able to decrypt it, and vice-versa). The two implementations must be done in a different language, using different libraries. This will aid in revealing and eliminating implementation-specific errors, which will help in ensuring that the implementations are correct.

Graduate (CISC 870) students must complete their projects individually.

Deliverables

The project is worth 25% of your final grade, and consists of the following three deliverables.

- Proposal (10%)
- Presentation (10%)

- Final report and implementation, including a link to a Github repository containing all associated code (80%)

More details will be provided on each of these deliverables.

Your proposal should contain the following:

- **Topic area and problem statement:** The general area and the specific goal that you set out to achieve (in a few sentences).
- **Expected results:** A description of the results/outcomes/contributions that you expect to achieve from completing the project (in a few sentences).
- **Primary resources:** Academic and/or non-academic references and tools, software libraries, or hardware (where applicable) that will serve as the starting point and that will play a key role in helping you complete your project. List the resources and in one or two sentences each briefly describe each item, how it relates to your project, and how you plan to make use of it.

A template/structure for the final report will be provided. However, as a general structure, the final report should document the following aspects of your project:

- **Topic area and problem statement:** The general area and the specific goal that you set out to achieve.
- **Background and related work:** A survey of existing work that is relevant and/or helpful to solving your problem. May include academic and/or non-academic sources (graduate students must include academic sources). Describe what is unique about your specific goal compared to other existing work within the same area. This section should be more broad/general.
- **Tools and libraries used.** Identify and describe all resources/tools/software libraries/hardware that you used.
- **Detailed overview/discussion of what you did.** For implementation-based projects, this will involve describing the methodology and techniques you employed (with a level of detail that allows a reader to reproduce your work) and a suitable evaluation, e.g., a thorough assessment of how your implementation withstands relevant attacks. For research-based projects, this will involve a detailed comparative analysis and evaluation of different techniques that demonstrates **in-depth** knowledge of at least four academic papers. This **must** be more than just a summary, i.e., you must offer your own original comparison and insights.
- **Concluding remarks.** This may include (i) discussion of the limitations of your work and more broadly of the field, (ii) open problems that need to be solved to ameliorate the limitations, and (iii) what you learned from the project.

The final report should be typed up in LaTeX and should be 5-7 pages in length using the following ACM template: https://www.overleaf.com/project/61d3e9906be73d0682ba8e98

Note that the report for research-focused topics and for group projects are expected to closer to the maximum length, whereas implementation-focused topics may be shorter (as long as all the requirements stated above are fully met). Graduate students are expected to deliver a more substantial project, compared to undergraduate students.