Tópicos Avançados em Ciência da Computação I:
Introdução à Teoria de Códigos para Criptografia Pós-Quântica
Prof. Daniel Panario

Lista de Projetos Finais
Entrega: Segunda Feira 3 de fevereiro de 2020
Valor no curso: 60% (apresentação oral 25%; projeto escrito 35%)

The following is a list of some possible topics for the final course project. You can choose topics outside this list; in this case, you must talk with me and we should agree on the project. I strongly suggest you start your search for a topic that fits your interests as soon as possible.

The kind of topics in the list are mainly theoretical but you may consider implementations too. Indeed, a project involving both components (some implementations together with some theoretical explanations) could be very interesting. However, if a topic is essentially an implementation of some algorithm, then it must include a report explaining how and why the program works, and must contain well-justified data testing.

A portion of the marks go to how your project is written and organized. I suggest you consider the following scheme: include a title with an abstract. In a first section, explain the problem you are addressing, the background (if needed), and clearly state your results and conclusions. No proof of theorems or programming code must appear in the first section. Then, describe the problem, the method you used (if applicable), how and why it works, and tables summarizing your experiments (if applicable) with clear explanations of the results. Finally, a list of references should appear. Programs (if applicable) should appear in an appendix.

Of course, there is no need of new results, but if you do have something that is new, explicitly point this out.

Possible main references for most of the topics are the webpages in the NIST standardization competition. In general, this is intended as a starting point for the search but in some cases is self-contained. You should consult the instructor to clear out doubts, suggest lines of action, help you on decisions about the topic, etc. Just come to talk to me or send me mail and we talk.

The project must be your own work. In particular, you **must cite** everything you are taking from the literature or internet. You can take proofs, explanations, etc, from papers and books but the final writing must be only yours. One possible way to enhance (and show) your understanding of some work is giving new proofs of results, filling some missing steps in theorems, adding examples, and so on.

You must have a project topic decided by Sunday January 19, 2020. That will ensure that everything is in order with your project. Send me email before Monday 20 letting me know your topic; we can talk in person on Monday 20, if needed. Include two or three paragraphs about your topic; this will help you start thinking on the problem.

By Friday January 24, 2020, a two/three pages extended abstract should be submitted to me. The oral presentation (20 minutes in total; 15 lecture plus minutes for questions and short break) will be on that day; your slides should also be handed on that day. The final paper (approximately 10-15 pages) is due on **Monday February 3, 2020** by mail.

A potential list of topics for final project is below. When there is no reference to a particular NIST code-based PQC proposal, then the topic applies to any of the seven proposals:

Bike, Classic McEliece, HQC, LEDAcrypt, NTS-KEM, Rollo and RQC.

- Security analysis of one of the proposals (hardness of underlying problem, known attacks, etc).
- Comparison of choice of parameters between two (or at most among three) of the proposals.
- Comparison of contributed implementations between two (or at most among three) of the proposals.
- Probabilistic analysis of the decryption failure rate of one of the proposals.
- Implementing the decoding algorithm of one of the proposals.
- Comparison of LEDAcrypt and Bike (LDPC/MDPC).
- Comparison of Rollo and RQC (rank metric).
- Comparison of Classical McEliece and NTS-KEM (McEliece versions).
- Analysis of BCH codes and its decoding in HQC.
- Timing side-channel attacks on the error locator polynomial and countermeasures.
- And so on. . ..