School of Mathematics and Statistics, Carleton University
MATH 4801/5609 Topics in Combinatorics: Post-Quantum Cryptography, Winter 2024

Instructor: Daniel Panario
Email: daniel@math.carleton.ca
http://www.math.carleton.ca/∼daniel

Day and time of course: Tuesdays and Thursdays 14:25 - 15:55.
Room: Southam Hall 317.

Office hours: Tuesdays 10:05 - 10:55 in HP4372.

Textbook: there is no textbook. A main source for the cryptographic applications is the main webpage of the NIST standardization competition:

`https://csrc.nist.gov/Projects/Post-Quantum-Cryptography`

In particular the following pages:

`https://csrc.nist.gov/Projects/post-quantum-cryptography/round-4-submissions`

`https://csrc.nist.gov/Projects/pqc-dig-sig/round-1-additional-signatures`

We plan to also use material from the following texts:

Post-Quantum Cryptography by Daniel J. Bernstein, Johannes Buchmann and Erik Dahmen (editors), Springer, 2009.

Finite Fields by Rudi Lidl and Harald Niederreiter, Cambridge Univ. Press, 1997.

CryptoSchool by Joachim von zur Gathen. Springer, 2015.

The Theory of Error-Correcting Codes by F. Jessie MacWilliams and Neil J.A. Sloane, North-Holland, Elsevier Science, 1977.

Prerequisites: mathematical maturity is recommended. Although not required, previous knowledge of finite fields and coding theory could be helpful, as well as undergraduate courses in abstract algebra, in cryptography and in number theory.

Course Objective: The main objective of this course is to study the main concepts, methods and results that play a central role in Post-Quantum Cryptography (PQC). We are guided by the applications of these concepts to cryptographic methods in the NIST (National Institute of Standards and Technology) standardization competition, currently in progress. The material we plan to cover in each lecture is below.

Evaluation: There will be two assignments (total 30%), 5 short quizzes (4% each), and a project that includes an oral presentation and a written project (total 50%).

Each quiz has two problems worth 50% per question; each problem has three possible outcomes: essentially correct (50%); some work done but far from totally correct (25%); or essentially nothing was done (0%). Hence, each quiz outcome is 100% (4 marks), 75% (3 marks), 50% (2 marks), 25% (1 mark), or 0% (0 marks). The five quizzes will be on Weeks 3, 5, 7, 9 and 11; they will be given after Tuesday class and must be uploaded before the beginning of the following Thursday class.

The 1st assignment will be handed out on January 30 and it is due on March 5; that day the 2nd assignment will be given that is due on April 2.

There is also a project (worth 50%) formed by three parts: a short introduction to the chosen project (worth 5%, about 2 to 3 pages, due on Thursday February 29), an oral presentation (worth 20%, with date to be arranged later but possibly on the week of April 8-12), and a final written project (worth 25%, about 15-20 pages, due after the talk, around Friday April 12). We will comment about the final project, and suggest potential topics, just before reading week. There is no final exam.

Academic Accommodation

You may need special arrangements to meet your academic obligations during the term. For an accommodation request the processes are as follows:

Pregnancy obligation: write to me with any requests for academic accommodation during the first two weeks of class, or as soon as possible after the need for accommodation is known to exist. For more details visit the Equity Services website.

Religious obligation: write to me with any requests for academic accommodation during the first two weeks of class, or as soon as possible after the need for accommodation is known to exist. For more details visit the Equity Services website.

Academic accommodations for students with disabilities: The Paul Menton Centre for Students with Disabilities (PMC) provides services to students with Learning Disabilities (LD), psychiatric/mental health disabilities, Attention Deficit Hyperactivity Disorder (ADHD), Autism Spectrum Disorders (ASD), chronic medical conditions, and impairments in mobility, hearing, and vision. If you have a disability requiring academic accommodations in this course, please contact PMC at 613-520-6608 or pmc@carleton.ca for a formal evaluation. If you are already registered with the PMC, contact your PMC coordinator to send me your Letter of Accommodation at the beginning of the term, and no later than two weeks before the first in-class scheduled test or exam requiring accommodation (if applicable). After requesting accommodation from PMC, meet with me to ensure accommodation arrangements are made.

Tentative lecture schedule

This weekly outline is subject to change depending on the progress of the course.

	Dates	Topics
1	Jan. 9-11	Introduction; PQC and NIST standardization competition. McEliece cryptosystem. Finite fields revision.
2	Jan. 16-18	Finite fields revision.
3	Jan. 23-25	Cryptographic notions.
		Quiz 1.
4	Jan. 30 - Feb. 1	Introduction to coding theory. Cyclic codes.
		Assignment 1 out.
5	Feb. 6-8	BCH codes. NIST proposal: HQC.
		Quiz 2.
6	Feb. 13-15	LDPC codes and bit-flipping decoding.
	Feb. 20-22	Winter break, no classes.
7	Feb. 27-29	NIST proposal: BIKE. Goppa codes.
		Quiz 3.
8	Mar. 5-7	NIST proposal: Classic-McEliece. Niederreiter cryptosystem. Gabidulin and rank metric codes.
		Assignment 1 in; Assignment 2 out.
9	Mar. 12-14	Lattice-based cryptography. GGH, LWE and NTRU.
		Quiz 4.
10	Mar. 19-21	NIST proposal: Crystals Kyber. Digital signatures.
11	Mar. 26-28	Multivariate cryptography. HFE cryptosystem. Oil and Vinegar, Unbalanced Oil and Vinegar (UOV).
		Quiz 5.
12	Apr. 2-4	NIST proposals: UOV/TUOV and WAVE. **Assignment 2 in.**
13	Apr. TBD	Student oral presentations. Final project deadline.