Carleton University
School of Mathematics and Statistics
MATH 4801/5609 Topics in Combinatorics: Finite Fields in Post-Quantum Cryptography
Winter 2022

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

Day and time of course: Tuesdays and Thursdays 13:05 - 14:25, Online. **Hybrid, on Zoom:** synchronous on Tuesdays, and asynchronous on Thursdays; recordings will be provided.

Office hours: Tuesdays 9:05 - 9:55, Online.

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`

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 University Press, 1997.

Handbook of Finite Fields by Gary Mullen and Daniel Panario, Chapman Hall/CRC, 2013.

Modern Computer Algebra by Joachim von zur Gathen and Jürgen Gerhard, Cambridge University Press, 1999.

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.

Signal Design for Good Correlation by Solomon W. Golomb and Guang Gong, Cambridge University Press, 2005.

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 of finite fields that play a central role in Post-Quantum Cryptography (PQC). We are guided by the applications of these finite fields 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 40%), 4 short quizzes (2.5% 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%, 75%, 50%, 25%, or 0%. The four short quizzes will be tentatively given at the end of a Tuesday class and must be returned before the beginning of the immediately following Thursday class, on weeks 4, 6, 8 and 10.

The first assignment will be tentatively given on January 25 and it is due on March 1st, after reading week. The second assignment should be given on March 1st and it is due on March 29.

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

Tentative lecture schedule

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

	Dates	Topics
1	Jan. 11-13	Introduction; PQC and NIST standardization competition. McEliece cryptosystem. Finite fields revision.
2	Jan. 18-20	Coding theory revision, linear codes, syndrome decoding, bounds. LDPC codes and bit-flipping decoding.
3	Jan. 25-27	Cyclic codes; BCH, Reed-Solomon and Reed-Muller codes. **Assignment 1 out.**
4	Feb. 1-3	Quasi-cyclic codes. Cryptographic concepts. **Quiz 1.**
5	Feb. 8-10	NIST proposal: BIKE. Information set decoding.
6	Feb. 15-17	BCH decoding and error locator polynomial. NIST proposal: HQC. Goppa codes. **Quiz 2.**
	Feb. 22-24	Winter break, no classes.
7	Mar. 1-3	NIST proposal: Classic-McEliece. Niederreiter cryptosystem. **Assignment 1 in; Assignment 2 out.**
8	Mar. 8-10	Gabidulin and rank metric codes. **Quiz 3.**
9	Mar. 15-17	Introduction to lattice-based cryptography.
10	Mar. 22-24	NTRU cryptosystem. NIST proposal: NTRU prime. **Quiz 4.**
11	Mar. 29-31	Multivariate cryptography. HFE cryptosystem. Digital signatures. **Assignment 2 in.**
12	Apr. 5-7	Oil and Vinegar, Unbalanced Oil and Vinegar. NIST proposal: Rainbow.
13	Apr. 12	Student oral presentations. Final project deadline.

Academic Accommodation

You may need special arrangements to meet your academic obligations during the term. For more details visit the Equity Services website. 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.

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.

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. Please consult the PMC website for the deadline to request accommodations for the formally-scheduled exam (if applicable).