Mathematics 4801/5609 Topics in Combinatorics: Finite Fields in Post-Quantum Cryptography

Fall 2020, Math 4801/5609
School of Mathematics and Statistics, Carleton University

Instructor: Daniel Panario
Office: #4372 HP, **Tel:** (613) 520 2600 (Ext. 2159)
Email: daniel@math.carleton.ca
Lectures: Tuesdays 14:35-15:55 and Thursdays 14:35-15:55. **Room:** online
Office hours: Tuesdays 11:00-12:00, or by appointment (send me mail or talk with me).

General Information

- **Course goals**: 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.
- **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.
- The material we plan to cover in each lecture is below.
- **Textbook:** there is no textbook. A main source for the cryptographic applications is the main webpage of the NIST standardization competition.
  We plan to also use material from the following texts:
  - Post-Quantum Cryptography, Daniel J. Bernstein, Johannes Buchmann and Erik Dahmen (editors), Springer, 2009.
  - Finite Fields, Rudi Lidl and Harald Niederreiter, Cambridge University Press, 1997.
  - Handbook of Finite Fields. Gary Mullen and Daniel Panario, Chapman Hall/CRC, 2013.
  - Modern Computer Algebra, Joachim von zur Gathen and Jürgen Gerhard, Cambridge University Press, 1999.
  - CryptoSchool, Joachim von zur Gathen. Springer, 2015.
  - The Theory of Error-Correcting Codes, F. Jessie MacWilliams and Neil J.A. Sloane, North-Holland, Elsevier Science, 1977.
  - Signal Design for Good Correlation, Solomon W. Golomb and Guang Gong, Cambridge University Press, 2005.
- **Classes begin:** Thursday, September 10, 2020.
  Classes end: Thursday, December 10, 2020.
  Fall break: October 26-30, 2017.
- **Evaluation:**
  There will be three assignments (total 40%), 5 short quizzes (2% each), and a project that includes an oral presentation and a written project (total 50%).

  Each quiz is evaluated as 2 marks (essentially correct), 1 (some work done but far from totally correct) and 0 (not done, or essentially nothing was done). The short quizzes are given at the end of Tuesday class and must be returned before the beginning of Thursday class on weeks 2, 4, 6, 8 and 10.

  The tentative schedule of assignments is below.

Assignment	Hand-out Date	Due Date	Worth
1	September 29	October 20	15%
2	October 20	November 10	15%
3	November 10	December 1	10%

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 November 5), an oral presentation (worth 20%, on the week of December 7-11), and a final project (worth 25%, about 15-20 pages, due on Friday December 11). We will comment about the final project, and suggest potential topics, just before reading week. There is no final exam.

- **Withdrawal:** The last day for withdrawal from the course without academic penalties is the last day of classes.
- **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 or religious obligation:** Write 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, see the Student Guide.
  - **Students with disabilities requiring academic accommodations:** Register with the Paul Menton Centre for Students with Disabilities (PMC) for a formal evaluation of disability-related needs. Documented disabilities include but are not limited to mobility/physical impairments, specific Learning Disabilities (LD), psychiatric/psychological disabilities, sensory disabilities, Attention Deficit Hyperactivity Disorder (ADHD), and chronic medical conditions. Registered PMC students are required to contact the PMC every term to have a Letter of Accommodation sent to the Instructor by their Coordinator.

Tentative lecture schedule (subject to change)

WEEK	DATES	TOPICS
0	Sep. 10-11	Introduction to the course. PQC and NIST standardization competition. McEliece and Niederreiter cryptosystems.
1	Sep. 14-18	Finite fields revision; fundamental properties; polynomials; arithmetic.
2	Sep. 21-25	Introduction to coding theory. Linear codes. Syndrome decoding. Bounds. **[Q1]**
3	Sep. 28 - Oct. 2	LDPC codes. Bit-flipping decoding. Cyclic codes. **[A1 out]**
4	Oct. 5-9	Cyclic codes (cont). BCH, Reed-Solomon and Reed-Muller codes. **[Q2]**
5	Oct. 12-16	Quasi-cyclic codes. Cryptographic concepts. NIST proposals: BIKE and LEDAcrypt. Information set decoding.
6	Oct. 19-23	BCH decoding and error locator polynomial. NIST proposal: HQC. Goppa codes. **[A1 in/A2 out; Q3]**
~	Oct. 26-30	READING WEEK
7	Nov. 2-6	NIST proposal: Classic-McEliece. Gabidulin and rank metric codes. **[Short project deadline.]**
8	Nov. 9-13	Introduction to lattice-based cryptography. NTRU cryptosystem. **[A2 in/A3 out; Q4]**
9	Nov. 16-20	NIST proposal: NTRU prime. Introduction to Groebner bases.
10	Nov. 23-27	Multivariate cryptography. HFE cryptosystem. Digital signatures. **[Q5]**
11	Nov. 30 - Dec. 4	Oil and Vinegar, Unbalanced Oil and Vinegar. NIST proposal: Rainbow. **[A3 in]**
12	Dec. 7-11	**[Student oral presentations. Final project deadline.]**

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