Proposed Directed Studies
Applications of finite fields
Fall 2013

Instructor David Thomson

Email dthomson@math.carleton.ca

Meeting times Tuesday 18:00-21:00 in HP 4369

Overview

The goal of this course is to examine the applications of finite fields, particularly in secure and efficient computing and communications systems. As motivation, we will explore the use of finite fields in symmetric- and asymmetric-key cryptography. We will also focus on the algebraic and number-theoretic problems stemming from the design and analysis of cryptosystems, which are in-use today.

Prerequisite

General knowledge of groups, rings and fields (MATH 3106 and MATH 3158, or equivalent) is strongly recommended. In particular, we will assume basic knowledge about properties of finite rings and finite fields. Familiarity with elementary number theory and computer science (e.g., basic complexity theory and some programming ability) will be helpful. Some relevant background may be provided, as needed.

We will not assume any particular previous knowledge of engineering principles of cryptography.

Recommended reference

Handbook of Applied Cryptography, A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, CRC Press (1996). Available online at: http://cacr.uwaterloo.ca/hac/

The recommended reference will be augmented by readings from the literature, proposed on a per-topic basis.

Format

The course will be run in a seminar style, and will be held either one day per week for 150 minutes or twice weekly for 75 minutes, each, depending on availability.

At the beginning of each major area, the instructor will give an overview of the topics to be covered. At the end of the each week, the instructor will provide a suggested reading list for the following week's topic(s). The student will be responsible for preparing a presentation of the material for the following week. The presentation may consist of any combination of the following elements: a description of the technical details of the topic, the active areas of research, the state-of-the-art, ideas for future research or other criteria to be decided concurrently by the student and the instructor. The course preparation portion of the evaluation will be determined by the readiness of the student on a per-week basis.

Evaluation

- Final project 50% (to be completed during the exam break)
- Course preparation 30%
- Assignments 20%

Assignments

Two assignments will be given at approximately the 1/3 and 2/3 mark of the course. The assignments will be comprehensive, and will encompass the material covered to that point. The assignments should take approximately 2 weeks to complete, and will be evaluated on completeness, technical quality, and composition.

Proposed topics and estimated schedule

Introduction:

Week 1: Terminology and concepts. Overview of information security and cryptography. Functions over finite groups/fields. Bird's-eye view of symmetric and asymmetric-key cryptography. Mathematical background, in particular complexity theory.

Suggested reading: 1.1-1.5, 2.3-2.4 (2.5-2.6 assumed as background)

Symmetric-key ciphers

Weeks 3-5:

- Confusion and diffusion;
- stream ciphers; LFSRs; linear complexity, Berlekamp-Massey algorithm;
- stream ciphers based on LFSRs; WG cipher.

Suggested reading: Chapter 6

- Block ciphers, substitution-permutation networks; classical ciphers;
- modern ciphers, e.g., AES, SAFER, RC5, GOST.

Suggested reading: 7.1-7.4, http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf#page=1

Criteria for good cipher design – engineering meets finite fields

Weeks 6-9

- Linear and differential cryptanalysis tutorial by Howard Heys: http://www.engr.mun.ca/~howard/PAPERS/ldc_tutorial.pdf
- Difference maps between finite groups; perfect non-linear and almost perfect non-linear functions; differential uniformity.

Suggested reading: selected readings TBD

- Boolean functions; discrete Fourier transform, nonlinearity; bent functions; relationship between bent functions and perfect non-linear functions.

Suggested readings from: C. Carlet, Boolean Functions for Cryptography and Error Correcting Codes, http://www.math.univ-paris13.fr/~carlet/chap-fcts-Bool-corr.pdf

- Conditions on symmetric-key ciphers. Detailed analysis of the Advanced Encryption Standard.

Suggested reading: R. Alvarez and G. McGuire, S-Boxes, APN Functions and Related Codes, Proceedings of the NATO Advanced Research Workshop on Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes, B. Preneel, S. Dodunekov, V. Rijmen and S. Nikove (eds.), Veliko Tarnovo, Bulgaria, 2008.

Implementation of finite fields for public-key cryptosystems

Weeks 10-11

- Public key cryptography; trapdoor functions; reference problems; RSA.

Suggested reading: 4.1, 4.4, 8.1-8.2.

- Implementations of finite fields in public-key systems; polynomial bases; polynomials of low-weight; normal bases; Gauss periods; rationale.

Suggested reading: NIST standards

Weeks >= 11 - Other topics

- Computations in finite fields; Karatsuba multiplication; Euclidean Algorithm; square-and-multiply exponentiation.

Suggested reading: Chapter 4 & Section 8.1 of ``J. Gerhard and J. von zur Gathen, Modern Computer Algebra (2nd ed.), Cambridge University Press, Cambridge, 2003.''

Final Project

The final project will comprise a written and an oral presentation. The project can either give significant background into an existing area -- including its significance, applications, and technical details in the author's own words and understanding; however ideally, it will comprise a literature review, background material and first thoughts/steps for the author to perform collaborative research on the topic. There is no specific length requirements for the written project, but it should be complete, clear and concise and will be graded on correctness and composition.

The oral component will comprise a thorough presentation of the key points of the written work and should be no less than 40 minutes and no more than one hour in length.

The final evaluation will be given as an overall score based on the clarity of each of the written and oral components.

Addendum: The students are **strongly** encouraged to present a poster at the *CMS Winter Meeting* in Ottawa on Sunday, December 8, *funding permitted.* Conference registration would also be included.

Some topics for the course project:

- Detailed history, analysis and cryptanalysis of the Enigma cipher.
- Non-Abelian bent functions and difference maps between non-Abelian finite groups.
- Applicable pseudo-random number generators.
- Fast-fourier transform for signal processing and finite field multipliers.
- Polynomial factorization methods over finite fields.
- Sub-exponential integer factorization.
- …others, more…