University of Waterloo  
Course Outline/Description of ECE 720-T2  
Winter 2020

Term and year of offering: Winter 2020

Course number and title: ECE 720-T2 Selected Topics in Cryptographic Computations

Lecture times, building and room number: 2:30-3:50, MTh, E5-5128. (Note: The first lecture is on Monday, January 6, 2020.)

Instructor:

Name: M. Anwar Hasan  
Office location: E7-5434  
Office hour: 4:00-5:00PM Thursdays or by appointment  
Contact: email: ahasan@uwaterloo.ca; phone: ext. 42868

Course description:

Finite fields. Computing in finite fields using standard and non-standard bases, and related high performance algorithms and architectures for cryptographic applications. Side channel analysis attack resistant computations.

Course objectives: At the end of the course you should be able to:

- Construct a multi-dimensional finite or Galois field and represent its elements with commonly used bases such as polynomial and normal bases
- Describe algorithms of various complexities for field arithmetic
- Devise hardware architectures of various space and time complexities for field arithmetic
- Describe algorithms of various engineering trade-offs for exponentiation and elliptic curve point multiplication used in RSA and ECC
- Have a good understanding of side channel analysis attack resistant computations

Course prerequisite: Bachelor degree in EE/CE/CS or equivalent, or instructor’s permission

Text and references:

- Text: There is no required text for this course. Copies of lecture slides will be available.
- References:
• Hankerson, Menezes and Vanstone, Guide to Elliptic Curve Cryptography (Chapters 2, 3 and 5)
• Menezes, van Oorschot and Vanstone, Handbook of Applied Cryptography (Chapters 2 and 14)
• Lin and Costello, Introduction to Error Control Coding (Chapters 2 and 6)
• McEliece, Finite Fields for Computer Scientists and Engineers (Chapters 2 and 8)
• Selected articles from IEEE Trans. on Computers and CHES proceedings.

Course topics:


Algorithms and architectures using standard representations-- Formulation of generalized finite field multiplication and optimization using field defining polynomials. Quadratic and sub-quadratic complexity multiplication algorithms. Digit level computations. Speed-ups using sub-field computations and look-up tables. Architectures for embedded and resource constrained systems. Systolic architectures. Multiplicative inversion using the almost inversion algorithm, solving equations over subfields, and using the extended Euclidean algorithm with polynomial updating up to the exact precision.


Evaluation: The course grade will be based on assignments, a project and a final examination which will be held during the Official Examination Schedule. The breakdown is as follows:

Assignments:  20%
Project:  30%
Final exam:  50%

Requirement for auditing the course: A student taking the course for audit is required to neither write the final exam nor do a project. For successful auditing, the student however must obtain a combined score of 50% or more in the assignments.