ECE 699-001/DL1: Post-Quantum Cryptography

Spring 2024

Course description

A broad introduction to post-quantum cryptography (PQC), understood as a class of public-key cryptographic schemes capable of being implemented using traditional software and hardware but resistant to all known attacks using both quantum and classical computers. Topics include major types of public-key schemes, such as public key encryption, key encapsulation mechanisms (KEMs), and digital signatures. The course covers the mathematical background and basic underlying operations, such as polynomial multiplication, hash and eXtendable Output Functions, operations on matrices, and Gaussian elimination. Examples of schemes belonging to the following five PQC families are discussed: lattice-based, hash-based, code-based, multivariate, and isogeny-based. The focus is on the visual representation of algorithms and data structures and the efficient and secure implementations in software and hardware. Countermeasures against side-channel attacks and the use of PQC schemes in major security protocols are explored. State-of-the-art and expected progress in quantum computing and its threat to classical public-key algorithms, such as RSA and elliptic curve cryptography, are overviewed and analyzed.

Prerequisites:

ECE 476 or CYSE 476 or CS 487 or IT 466 or CS 587 or ECE 646 or permission of instructor

Instructor

Dr. Kris Gaj
The Nguyen Engineering Building (ENGR), room 3225
E-mail: kgaj@gmu.edu

Lecture

Thursday, 7:20-10:00 PM, Section 001: Innovation Hall, room 203, Section DL1: Zoom

Office hours:

Face-to-face: Thursday, 6:00-7:00 PM, or by appointment, ENGR 3225.
Using Zoom: *Please send an e-mail request or private Piazza request, including your availability in the form of a list of days and time slots suitable for you. I will select one particular day and starting time of the meeting, and I will send you the corresponding Zoom link.*
During the conference call, please make sure to have your camera on and the ability to share your screen.

Communication

Please use Piazza instead of e-mail for asking questions and holding discussions related to this class. Please submit all your homework and project reports using Blackboard by going to https://mymason.gmu.edu.

Tentative Schedule (subject to possible modifications)

No.	Subject	Date
1.	Introduction to Post-Quantum Cryptography. Organization of the Course.	01/18/2024
2.	Mathematical Background – groups, rings, and fields	01/25/2024
3.	Algorithms for fast multiplication of polynomials	02/01/2024
4.	Hash functions and eXtendable Output Functions. Random Sampling.	02/08/2024
5.	Module-Lattice-Based Key-Encapsulation Mechanism Standard (FIPS 203): ML-KEM a.k.a. CRYSTALS-Kyber	02/15/2024
6.	Module-Lattice-Based Digital Signature Standard (FIPS 204): ML-DSA a.k.a. CRYSTALS-Dilithium	02/22/2024
7.	Stateless Hash-Based Digital Signature Standard (FIPS 205): SLH-DSA a.k.a. SPHINCS+	02/29/2024
8.	**Midterm Exam**	03/14/2024
9.	Code-based key encapsulation mechanisms (KEMs)	03/21/2024
10.	Multivariate signature schemes	03/28/2024
11.	Isogeny-based cryptography	04/04/2024
12.	Side-channel analysis: Threats and countermeasures	04/11/2024
13.	Use of PQC in protocols. Cryptographic libraries and modules. Migration from classical to post-quantum cryptography.	04/18/2024
14.	State of the art in quantum computing. Shor's and Grover's algorithms.	04/25/2024
15.	**Final Exam (7:30-10:15 PM)**	**05/02/2024**

Homework

Homework assignments will be posted at least 7 days before a given assignment is due.

All solutions should be submitted through Blackboard in electronic form. When preparing your hand-drawn/hand-written solutions for submission, please use either a scanner app on your smartphone or a traditional scanner (often integrated with your printer). Please do not submit photos; they are usually hard to read and take up a lot of space. You can also use a tablet, such as an iPad, to write down and save your solutions directly in electronic form.

Each student can have an automatic 72-hour extension on one assignment (no questions asked) as long as the student informs the instructor in writing.

Any additional late assignments will earn a flat 20% grade deduction as long as they are completed within 7 days of the deadline.

For selected assignments, you will have an opportunity to submit a revised version of your solutions due a week after receiving your graded homework. Your final score for the assignment will be an average of your first and second scores.

Exams

All exams will be in-class. You will have an opportunity to prepare and use a cheat sheet.
You must not communicate with anybody by any means during the exam!

Project

The project can be done in a team of 1-3 students. Students can choose a project topic from a list of topics suggested by the instructor. They can also suggest a project topic by themselves. Projects can be of different types: software, hardware, analytical, and mixed. All types of projects are expected to involve some experiments and literature search. Students will be asked to write a project specification, deliver bi-weekly project reports, give a project presentation, and develop a comprehensive project report.
An individual project in this course can be used to fulfill the scholarly paper requirement.

Grading

Homework	15%
Project	35%
Midterms Exam	20%
Final Exam	25%
Quizzes	5%
Class & Piazza Activity:	up to 5% bonus
Best Project Awards:	up to 10% bonus

Literature

Supplementary Textbooks

- William Stallings, *Cryptography and Network Security: Principles and Practice*, 8th ed., Pearson, 2020
  - 14.3 Post-Quantum Cryptography Concepts
  - 14.4 Post-Quantum Cryptographic Algorithms
- Douglas R. Stinson and Maura B. Paterson, Cryptography: Theory and Practice, 4th ed., CRC Press, 2019
  - 9 Post-Quantum Cryptography

Draft Standards

- FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM)
- FIPS 204: Module-Lattice-Based Digital Signature Standard (ML-DSA)
- FIPS 205: Stateless Hash-Based Digital Signature Standard (SLH-DSA)
- Recommendation for Stateful Hash-Based Signature Schemes: NIST SP 800-208

Reports

- NISTIR 8413: Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process, 09/26/2022

Schools and Tutorials

- Summer School on Post-Quantum Cryptography 2017
- Executive School on Post-Quantum Cryptography 2017
- Post-Quantum Cryptography for Embedded Systems, by Tim Guneysu, CHES 2017, Taipei, Taiwan, 2017
- Isogeny-Based Cryptography in Hardware, by Reza Azarderaksh, CHES 2019, Atlanta, USA, 2019

Conferences and Workshops

- NIST PQC Standardization Conferences

Software Libraries

- PQClean – Portable implementations in C99
- pqm4 - Post-quantum crypto library for the ARM Cortex-M4
- libpqcrypto - library generated by the European PQCRYPTO project

Basic Course Technology Requirements

Activities and assignments in this course will regularly use the Blackboard learning system, available at https://mymason.gmu.edu. Students are required to have regular, reliable access to a computer and a stable broadband Internet connection (cable modem, DSL, satellite broadband, etc., with a consistent 1.5 Mbps [megabits per second] download speed or higher.

Activities in this course will regularly Zoom for office hours and project meetings. Therefore, students are expected to have a device with a functional camera and microphone. In an emergency, students can connect through a telephone call, but video connection is the expected norm.

Academic Integrity

The integrity of the University community is affected by the individual choices made by each of us. Mason has an Honor Code with clear guidelines regarding academic integrity. Three fundamental and rather simple principles to follow at all times are that: (1) all work submitted must be your own; (2) when using the work or ideas of others, including fellow students, give full credit through accurate citations; and (3) if you are uncertain about the ground rules on a particular assignment, ask for clarification. No grade is important enough to justify academic misconduct. Plagiarism is the equivalent of intellectual robbery and cannot be tolerated in the academic setting. If you have any doubts about what constitutes plagiarism, please see me.
For more information about the Mason Honor Code and about the Honor Committee, please visit the Office of Academic Integrity website (http://oai.gmu.edu).