Course Syllabus: Post-quantum Cryptography (In-Person), 2024
Department of Computer Science, Queens College, CUNY

Professor Dr.: Delaram Kahrobaei (delaram.kahrobaei@qc.cuny.edu)

1 Textbooks

- Jonathan Katz and Yehuda Lindell, *Introduction to Modern Cryptography* (3rd edition), (Chapman & Hall/CRC Cryptography and Network Security Series)(2020)
- Andrew M. Childs, *Lecture Notes on Quantum Algorithms* (2022), `https://www.cs.umd.edu/~amchilds/qa/qa.pdf`

2 Course Outline/Topics:

- Review on Mathematical Topics (Algorithmic Algebra, Number Theory), computational complexity
- Review for Public-key Encryption, Digital Signature
- Introduction to Quantum Computing: Shor's Algorithm, Grover's Search
- Post-quantum Cryptography under consideration by NIST and NSA
- Lattice-based Primitive
- Code-based Primitive
- Hash-based Primitive
- Multivariate-based Primitive
- Group-based primitive
- Quantum Cryptography: Quantum Key Distribution (QKD)
- AI cryptanalysis for Post-Quantum cryptosystems

2.1 Grading, Exams and Important Dates:

- Attendance is mandatory.
- First Day of Classes: January 29, 2024
- Mon. 04/22 – Tue. 04/30, 2024, No Class, Spring Recess
- May 15, 2024, Last Day of Classes.
- **Midterm** 50%.
- **Final** 50%.

2.2 Projects and Presentations

- Choose 4 members team.
- Choose one of the Digital Signatures submitted to NIST PQC Project from `https://csrc.nist.gov/Projects/pqc-dig-sig/round-1-additional-signatures`
- Send an email to Prof. Dr. Kahrobaei, with the Subject PQC Project, copying all team members, include the list of team members and write the name and link to your selected project by February 7th, 2024.
- March 4: Submit a 10 page manuscript of your chosen Scheme and send it by email copying all team members. Include slides for 20 minutes presentation, each team member has 5 minutes to present. Include the names and pictures of all team members in the first pages of your slides and mansucript.
- Presentation will be done through March 4–13, 2024
- Submit the final presentation on May 6th, and present during class, same format as the midterm. Presentations will be done from May 6th–May 15th.
- Submit a 20 page final manuscript final manuscript by May 15.

2.3 Grading Policy:

Grades are based solely on the knowledge you are able to demonstrate on exams and projects. Partial credit is only given to answers that make progress on a problem. Here is the grading curve:

- A 90+
- A- 80– 89
- B+ 75 – 79
- B 70–74

- B- 65 – 69
- C 60 – 64
- C- 50 – 59
- F 0 – 49

Your final numerical grade on an exam is the lowest such numerical grade that your letter grade corresponds to in the CUNY grading policy which you can find here: https://www.qc.cuny.edu/academics/supportprograms/advising/academic-and-grading-policies/Pages/Default.aspx. Your final grade in the course is simply the weighted average of your numerical grades according to the weights above. NOTE: ALL GRADES ARE FINAL! No changes will be made to exam grades as a curve is already applied.

IMPORTANT DATE: A grade of W does not impact your GPA, however you will need to retake the class as the department requires that all CS courses must be completed with a grade of at least C to get credit.

3 Blackboard and Announcements:

Make sure you can log in to Blackboard. If you cannot, please contact the Help Desk at 718-997-4444. Please familiarize yourselves with how Blackboard works. For example, you may wish to view https://keepteaching.qc.cuny.edu/i-need-help-with/video-conferencing. All major class announcements will appear on Blackboard in Announcements. Please regularly check the Announcements folder. You are each responsible for all class announcements made in lecture and posted to Blackboard - whether or not you are in attendance in the live class lecture. Bulk email messages will be rare. (The email addresses I will use for you are the ones in Blackboard. Make sure your Blackboard email address is updated. In addition, you should check and update your CUNYFirst email address.)

4 Email Communication:

All emails to me should be sent from your queens college email account to delaram.kahrobaei@qc.cuny.edu. I cannot answer emails that do not come directly from your queens college account. So please make sure that you can access your account. If you have issues with your account, contact the Help Desk at 718-997-4444 or helpdesk@qc.cuny.edu.

5 Office Hours:

Office hours are on Mondays and Wednesdays 12:00-1:30 PM. If you are planning to come, I request that you email me so I know in advance. It is also good if you could let me know what it is you'd like to discuss, that way I can best prepare the material to help you. In office hours you are free to discuss anything you are concerned about. I will hold office hours at SB A112.

6 Academic Integrity:

Academic dishonesty is prohibited in The City University of New York. Penalties for academic dishonesty include academic sanctions, such as failing or otherwise reduced grades, and/or disciplinary sanctions, including suspension or expulsion. See our guidelines at: `http://www.cs.qc.edu/index-1.html`. Everyone in the class should consider cheating as an attack on his or her personal investment to obtain a degree and his or her personal prospects for financial success. We all, myself included, have a responsibility to ensure that the name of our institution is recognized as a place that produces a high quality product, and those that end up moving forward without having learned the material endanger your job prospects as they wrongly present the quality of student we produce. NOTE: All cases of cheating, plagiarism, or unauthorized collaboration will be documented and taken up with the department and the Office of Academic Integrity. In the meantime you should read `https://www.cuny.edu/about/administration/offices/legal-affairs/policies-procedures/academic-integrity-policy/`. There you'll find everything you need to know about what you should not do and the procedures that will take place if cheating is suspected and found.

7 Changes to Syllabus:

I reserve the right to change portions of the syllabus as the class progresses. Most notably the topics that we cover may change time will dictate how much we will be able to cover. We will aim to cover all the topics mentioned.