CS/Ph 120 Quantum cryptography

Term: Fall 2019
Lectures: TBD
Instructor: Thomas Vidick
Office Hours: Tuesday 5-6pm, 207 ANB
TA: TBD. *OH*: TBD

Course description

This course is an introduction to quantum cryptography. The goal of the course is to give you the ability to understand at a conceptual as well as technical level what makes quantum cryptography different and exiting; what it is useful for and what are its limitations. Starting with the basics of quantum information and cryptography we will study fundamental tasks in quantum cryptography: quantum money, the quantum one-time pad, secret sharing, nonlocal games, and two-party tasks such as bit commitment, coin-flipping and oblivious transfer. By the end of the course you will be able to formally design, analyze and show security of cryptographic protocols that make use of quantum information to implement novel tasks with strong security guarantees.

Prerequisites: Ma 1b. CS 21, CS 38 or equivalent recommended. No background in quantum mechanics required, though Ph 2b and 12b can be helpful. This course is largely disjoint from CS 152 and can be taken independently from it.

Course information

Office hours and recitation: You are strongly encouraged to come to my office hours and to those held by the TA. My office hours are Tuesdays 5-6pm in my office, 207 ANB. You can come to office hours to discuss assignments, but not only for that. You can come to discuss anything related to the course: the material covered in class, the material not covered in class, your interest in the class, etc. You are also welcome to come in for advice on how to do well in the class.

Communication: Communication will be made in class and through Piazza.

Course TAs: TBD.

Evaluation

Evaluation in the course is based on a variety of assignment types. The bulk of the work will be proof-based assignments with an emphasis on mathematical rigor. These are complemented by programming assignments that allow you to practice with the implementation of quantum circuits and protocols, and reading assignments that encourage you to reflect on the broader context.

In addition to attending 3 hours of lecture weekly, students are expected to:

- *(5% of grade)* Attend lecture
- *(10% of grade)* Prepare for lecture by completing a small quiz or puzzle (weekly). You are allowed to skip up to 3 quizzes while still receiving full grade. The goal of the quizzes is to make sure every student is following the class, and that no one falls behind.
- *(40% of grade)* Turn in a bi-weekly homework set. There will be 4 sets. Each set will be 80% proof-based and involve a small programming component using Julia/Jupyter notebooks. Sets are due by Friday 5pm. Handwritten or latexed solutions are equally good. Grading will take into account clarity and rigor of exposition: make sure your solutions are presented appropriately and include complete proofs whenever required.
- *(15% of grade)* Complete a bi-weekly reading assignment. There will be 3 reading assignments. Each assignment will require you to read one or two short papers with historical significance in quantum cryptography, and turn in one or two pages of reflections on the paper (you will be given guiding questions). The goal of these assignments is to encourage you to take a historical perspective and reflect on deeper questions that go beyond the math. Grading will be generous: I hope you enjoy the readings!
- *(30% of grade)* Complete a project. This can be reading, research, or implementation-based. The project will lead to a report and an in-class presentation.

Indicative syllabus

See the course webpage for up-to-date information.

- Weeks 1-2: Introduction to quantum computing. Quantum money and attacks on it.
- Weeks 3-4: density matrices and CPTP maps. Quantum encryption and notions of security. The quantum one-time pad.
- Weeks 5-6: Measuring randomness. Nonlocal games and Guessing games.
- Weeks 7-8: Extractors and privacy amplification. Information reconciliation. The BB'84 protocol for quantum key distribution.

- Weeks 9-10: Security of BB'84 using guessing games. Two-party quantum cryptography.

Resources

Your main resource will be the lecture notes. A somewhat dated introductory textbook on quantum cryptography is Protecting Information: From Classical Error Correction to Quantum Cryptography by Loepp and Wootters. The book covers some topics from the class, but we will go further. For background, a good reference on quantum information is the book Quantum Computation and Quantum Information by Nielsen and Chuang.

Collaboration policy

See the collaboration table.

- The quizzes and reading assignments should be completed on your own: no collaboration. We will discuss those in class, and you are welcome to bring any questions you have there.
- The problem sets can be solved in collaboration with other students in the class (and I encourage it). But you should read and think about each problem alone for at least a few minutes before collaborating. *You must produce the final write-up for submission alone, without relying on notes of any kind from your discussions; your solution must depend solely on your own understanding.*
- It is ok to look up definitions online or whereever you find convenient. It is not ok to use solutions found online, in whole or in part. If by accident you find a solution to an assigned problem, or a problem that is close to an assigned problem, you should immediately put it aside. *Do not violate the honor code.* In case of uncertainty *ask.*
- In all cases where collaboration is allowed, you should indicate on your solution the name of your collaborator(s).