State University of New York Polytechnic Institute
CS 538 : Extended Private Computation

Instructor: Dr. Chen-Fu Chiang

Semester: Spring 2024
Time: MW 6:00 pm - 7:15 pm
Location: Kunsela Hall A129
Office Hours: MW (My office) : 2:00 pm - 4:00 pm

Office : Location: Kunsela C225 || Phone: (315) 792-7379
Email: chiangc@sunyply.edu (best way to reach me)
URL: http://www.cs.sunyit.edu/∼chiangc

References

1. Quantum Computation and Quantum Information ||Cambridge University Press, ISBN-10: 9781107002173
2. A Graduate Course in Applied Cryptograph (https://toc.cryptobook.us/book.pdf)

Useful Online Basic Reference & Lab for Lecture Notes

1. Foundations of Cryptography http://www.mit6875.org/
2. Quantum Algorithms - Andrew Childs (https://www.cs.umd.edu/∼amchilds/qa/qa.pdf)

Note

1. This is an introductory graduate course intended for beginning graduate students and upper level undergraduates. Fluency in algorithms, complexity theory and discrete probability are necessary. Mathematical maturity and an ease with writing mathematical proofs will be assumed starting from the first lecture. .
2. The quantum section of the course is self-contained.

Course Description

This is a more research oriented course that aims at binding private computation with quantum technology. The field of cryptography gives us a technical language to define important real-world problems such as security, privacy and integrity, a mathematical toolkit to construct mechanisms such as encryption, digital signatures, zero-knowledge proofs, homomorphic encryption and secure multiparty computation, and a complexity-theoretic framework to prove security using reductions. For example, cryptography is abuzz with solutions to long-standing open problems such as fully homomorphic encryption and software obfuscation that use an abundance of data for public good without compromising security. The course will explore the rich theory of cryptography all the way from the basics to the recent developments. Quantum information and computation exploits quantum mechanical rules to process information. As a new branch of interdisciplinary science, it has both fundamental and technological implications. We will select existing quantum algorithms, such as quantum walk, as secure encryption technique and explore its applications in private computation. Since quantum walk is a universal quantum computation framework, it implies the applications can be also adapted for other universal quantum computation frameworks.

Student Learning Outcomes

Upon completion of this course the student should be able to:

- Understand the Basics of Cryptography and Private-Key
- Explain the State-of-the-Art Protocols in Secure Computation
- Understand modern Quantum Algorithms, escpeically in the Quantum Walk Framework
- Apply Cryptogrpahy and Private Computation into Quantum Algorithms

Topics

Each topic should last for 1 or 2 lectures, based on the progress in the class. The instructor will speed up or slow down the lectures according to students' understanding of the material. It is recommended that the students read the material (and the original papers) ahead before the lecture. Topics from 1 to 5 are the basic fundamentals. Topics from 6 to10 are the more advanced theoretical quantum algorithms. Topics from 11 to 16 are the state-of-the-art NISQ techniques and its applications.

seq #	Topics	seq #	Topics
1	Introduction to Cryptography	2	Secure Commnication
3	Shannon's Lower Bound	4	Pseudorandom Generators (PRG)
5	PRG Imply Secret-Key Encryption	6	Message-Authentication Codes (MAC)
7	Secure Computation	8	Secure Two-Party Computation Protocol
9	Secure Multi-Party Computation	10	Yao's Garbled Circuits
11	Fully Homomorphic Encryption Part I	12	Fully Homomorphic Encryption Part II
13	Discrete Time Quantum Walk	14	Continuous Time Quantum Walk
15	Quantum Homomorphic Encryption	16	Private Quantum Computation

Grading (Tentative)

The lecture format will be the basic mechanism used in the course. Computer demonstrations in the classroom will be used whenever appropriate. Assessment of student performance will use a criterion-referenced model which will include written assignments (30%), regular examinations (midterm 25%), presentation along with a short report regarding either quantum algorithms or implementation via quantum programming languages (20%), and a comprehensive final exam (25%). **Late assignment will not be accepted unless you have made prior arrangements with me**. The acceptable format of your solution will be specified in the assignment. All examinations are closed-book. Percent and Grade :
89.5-100 A 79.5-89.5 B 69.5-79.5 C 59.5- 69.5 D Below 59.5 F
(+/- modifiers will also be used ; for instance, [95.5-100]: A+, [92.5-95.5): A, [89.5-92.5): A-)

Attendance Policy

Attendance and active class participation are required. Be prepared to participate by asking and answering questions during class meetings. Please send me an email if you know you have to miss a class.

Academic Integrity/Policy

Plagiarism and Cheating of any kind on an examination, quiz, or assignment will result at least in an F for that assignment (and may, depending on the severity of the case, lead to an F for the entire course). I will assume for this course that you will adhere to the academic creed of this University and will maintain the highest standards of academic integrity. In other words, do not cheat by giving answers to others or taking them from anyone else. The code of academic conduct is detailed on the SUNY Poly student handbook. Make-ups are only given under extreme circumstances. I will also adhere to the highest standards of academic integrity, so please do not ask me to change (or expect me to change) your grade illegitimately

or to bend or break rules for one person that will not apply to everyone.

Plagiarism Warning

The work you submit must be your own. You will not receive credit for work which is not your own. You may ask others (classmates/friends/instructors) for advice or help regarding the subject matter of a problem set. However, your answers and the actual design, coding, entry, and running of your programs must represent your own work. All sources of ideas that are used in any way (quoted, paraphrased, or summarized), including ideas taken from the text, must be acknowledged in problem set program documentation. Failure to provide proper attribution constitutes academic dishonesty, and it will result in a failing course grade. Substantially identical program submissions by multiple students, even with attribution, may result in a failing course grade to all who submit the same program. Submitting a program written by someone else, even with attribution, is strictly prohibited and will result in a failing course grade. Students are further reminded that it is their responsibility to take reasonable precautions to prevent copying of their work by other students and that there are now criminal penalties for computer trespass and computer tampering.

Cancellation of Classes Due to Inclement Weather or Other Emergency

SUNY Poly has a 24-hour hotline to inform students, faculty and staff when severe winter weather prompts the cancellation of all classes. On-campus, you can call the "Snowline" by dialing ext. 7669 ("SNOW"). Off-campus, Snowline can be reached by calling 315-792-7385. Snowline cards are available at various locations on campus. In the event of severe weather, Snowline will announce only the cancellation of ALL classes. The cancellation of all classes will also be posted online, at sunypoly.edu, and will be broadcast on radio and television stations in the Utica-Rome, Syracuse, and Albany areas. Individual class cancellations are always available at sunypoly.edu/apps/canceled_classes .

Accommodations for Students with Disabilities

Your access in this course is important to me. In compliance with the Americans with Disabilities Act of 1990 and Section 504 of the Rehabilitation Act, SUNY Polytechnic Institute is committed to ensuring comprehensive educational access and accommodations for all registered students seeking access to meet course requirements and fully participate in programs and activities. Students with documented disabilities or medical conditions are encouraged to request these services by contacting Student Accessibility Services (SAS) or filling out the Disability Declaration form. Please note, you must provide documentation to SAS and meet with staff before receiving accommodations. Please do this as early as possible so that we have adequate time to arrange your approved academic accommodation/s. Once SAS creates your accommodation plan, it is your responsibility to provide me a copy of the accommodation plan. If you experience any access barriers in this course, such as with printed content, graphics, online materials, etc., reach out to me or Accessibility Services right away. For information related to these services or to schedule an appointment, please contact the SAS using the information provided below.

Office of Student Accessibility Services
SAS@sunypoly.edu
(315) 792-7310
Peter J. Cayan Library, L112