CSCI 575: Quantum Computing and Quantum Cryptography

Units: 4
Lecture Time: 1hr50min, twice weekly

Instructor: Ming-Deh Huang
Office: SAL 314
Office Hours: TBD
Contact Info: mdhuang@usc.edu, x4783.

Course Description

For decades considered a controversial mathematical and theoretical model of Physics, quantum mechanics is now the basis upon which revolutionary computing devices and communication systems are being designed and developed. Quantum computing has emerged as a prominent research area with tremendous potential for practical applications. The quest for practical large scale quantum computation and information processing has become more pressing and competitive. This course serves as an introduction to the fundamental ideas and techniques in quantum computing and quantum cryptography. Background material in mathematics, computer science and quantum mechanics is discussed at a level suitable for beginning graduate students in the three disciplines. Our exploration will be guided by the following questions: What are the quantum mechanical principles as they apply to computation? How is quantum computation different from or better than classical computation? What does it take to realize quantum computation? Topics of study and investigation include quantum Fourier sampling, with applications to search, period finding, factoring and discrete logarithm problems, and quantum key distribution, with connection to EPR paradox and Bell's inequalities.

Learning Objectives

After completing this course, students will be able to
- Design and analyze quantum circuits and algorithms
- Formulate and define cryptographic security in a quantum mechanical setting
- Design and analyze cryptographic protocols based on quantum mechanic principles
- Demonstrate knowledge of contemporary research in quantum computing and quantum cryptography
- Apply knowledge of quantum mechanics in addressing challenges in computing and cryptography

The objectives will be achieved through the combination of lectures, discussions, readings (textbook and selected papers), homework assignments, midterm paper and final project (paper and presentation).

Recommended Preparation: CSCI 570, and knowledge of linear algebra at the level of EE 510 (preferred) or MATH 225.

Course Notes

Lecture slides and other class information will be posted on Blackboard.

Required Readings

Textbook: Quantum computation and quantum information, Michael A. Nielsen and Issac L. Chuang. Cambridge. ISBN 10: 1107002176 ISBN 13: 9781107002173

Supplementary Materials

Selected papers.

Description and Assessment of Assignments

About 5 homework assignments will be given throughout the semester. There will be midterm exam, which consists of a problem set and a midterm paper on an assigned topic. There will be a final project which includes paper and presentation.

Grading Breakdown

Assessment Tool (assignments)	% of Grade
Homework	40
Midterm problem set	20
paper	10
Final project abstract	5
paper+presentation	25
TOTAL	100

Assignment Submission Policy

Assignments are submitted through Blackboard on or before due times.

Course Schedule: A Weekly Breakdown

	Topics/Daily Activities	Readings/Preparation	Deliverables
Week 1	What is in a bit? The classical vs quantum model of computing	1.1, 1.2	Homework 1 posted
Week 2	EPR paradox, Bell's inequality and quantum cryptography – First discussion	Papers on EPR and Bell theorem	Homework 1 due
Week 3	Quantum algorithms	1.3, 1.4	Homework 2 posted
Week 4	Quantum algorithms	4.1-4.4	Homewok 2 due
Week 5	Quantum circuit complexity	4.5-4.7, Papers	Midterm paper abstract due
Week 6	Quantum Fourier sampling	5.1, 5.2	Homework 3 posted
Week 7	Group theory, Number theoretic computation	Appendix 2 and 4	Homework 3 due
Week 8	Quantum order finding, factoring, discrete logarithms, Hidden subgroup problems (HSP)	5.3, 5.4, Papers (HSP)	Midterm paper due
Week 9	Quantum search Quantum random walk	6.1, 6.2 Papers	Homework 4 posted
Week 10	Cryptography	Appendix 5	Homework 4 due
Week 11	Quantum key distribution (QKD) and bit commitmemnt	12.6 Papers	Final paper abstract due
Week 12	Further topics on quantum cryptography (Encryption, garbled circuits, etc)	Papers	Homework 5 posted

Week 13	Quantum computers	7.1, 7.2, 7.4, 7.6	Homework 5 due
Week 14	Hamiltonian simulation Quantum linear system sproblem (HHL algorithm)	Papers	Final paper due
Week 15	Presentation		Paper presentation
FINAL	Final presentation and conclusion		Refer to the final exam schedule in the USC *Schedule of Classes* at classes.usc.edu.

<u>**CSCI 575 Project**</u>

Course project: the purpose of the class project is for you to explore recent theoretical results or emerging practical applications of quantum computation and quantum cryptography. You are expected to conduct literarure search, present your interpreatation and analysis of existing works, and conclude by a discussion of prospects and challenges for future research. Working as a group is permitted if the project is large enough to justify this. A team can consist of no more than 2 persons.

Project Timeline:
- Week 11: Proposal due
- Week 14: Project paper due
- Final's week: Project presentation

Sample projects:
- Secure multi-party quantum computation
- Quantum machine learning

Project Presentation: The presentation should be approximately 15 minutes in duration and should cover all aspects of the project development, including motivation, recent works, your analysis and conclusion. You may use PowerPoint or LaTeX or similar. Typically plan on one slide per minute; content should be phrases in bullets, not prose. Do not read word-for-word from your slides!

Final Report: The project final report documents the motivation of the research topic, the formulation of the research issues, discussion and analysis of recent works, your observations, conclusions and references. The main text of the report will typically be 8–10 pages.

Grading breakdown: All aspects of the project combined are 30% of the semester grade, with a breakdown:
- Proposal: 5%
- Final report: 15%
- Presentation: 10%

Statement on Academic Conduct and Support Systems

Academic Conduct:

Plagiarism – presenting someone else's ideas as your own, either verbatim or recast in your own words – is a serious academic offense with serious consequences. Please familiarize yourself with the discussion of plagiarism in SCampus in Part B, Section 11, "Behavior Violating University Standards" policy.usc.edu/scampus-part-b. Other forms of academic dishonesty are equally unacceptable. See additional information in SCampus and university policies on Research and Scholarship Misconduct.

Students and Disability Accommodations:

USC welcomes students with disabilities into all of the University's educational programs. The Office of Student Accessibility Services (OSAS) is responsible for the determination of appropriate accommodations for students who encounter disability-related barriers. Once a student has completed the OSAS process (registration, initial appointment, and submitted documentation) and accommodations are determined to

be reasonable and appropriate, a Letter of Accommodation (LOA) will be available to generate for each course. The LOA must be given to each course instructor by the student and followed up with a discussion. This should be done as early in the semester as possible as accommodations are not retroactive. More information can be found at osas.usc.edu. You may contact OSAS at (213) 740-0776 or via email at osasfrontdesk@usc.edu.

Support Systems:

Counseling and Mental Health - (213) 740-9355 – 24/7 on call
studenthealth.usc.edu/counseling
Free and confidential mental health treatment for students, including short-term psychotherapy, group counseling, stress fitness workshops, and crisis intervention.

National Suicide Prevention Lifeline - 1 (800) 273-8255 – 24/7 on call
suicidepreventionlifeline.org
Free and confidential emotional support to people in suicidal crisis or emotional distress 24 hours a day, 7 days a week.

Relationship and Sexual Violence Prevention Services (RSVP) - (213) 740-9355(WELL), press "0" after hours – 24/7 on call
studenthealth.usc.edu/sexual-assault
Free and confidential therapy services, workshops, and training for situations related to gender-based harm.

Office for Equity, Equal Opportunity, and Title IX (EEO-TIX) - (213) 740-5086
eeotix.usc.edu
Information about how to get help or help someone affected by harassment or discrimination, rights of protected classes, reporting options, and additional resources for students, faculty, staff, visitors, and applicants.

Reporting Incidents of Bias or Harassment - (213) 740-5086 or (213) 821-8298
usc-advocate.symplicity.com/care_report
Avenue to report incidents of bias, hate crimes, and microaggressions to the Office for Equity, Equal Opportunity, and Title for appropriate investigation, supportive measures, and response.

The Office of Student Accessibility Services (OSAS) - (213) 740-0776
osas.usc.edu
OSAS ensures equal access for students with disabilities through providing academic accommodations and auxiliary aids in accordance with federal laws and university policy.
USC Campus Support and Intervention - (213) 821-4710
campussupport.usc.edu
Assists students and families in resolving complex personal, financial, and academic issues adversely affecting their success as a student.

Diversity, Equity and Inclusion - (213) 740-2101
diversity.usc.edu
Information on events, programs and training, the Provost's Diversity and Inclusion Council, Diversity Liaisons for each academic school, chronology, participation, and various resources for students.

USC Emergency - UPC: (213) 740-4321, HSC: (323) 442-1000 – 24/7 on call
dps.usc.edu, emergency.usc.edu
Emergency assistance and avenue to report a crime. Latest updates regarding safety, including ways in which instruction will be continued if an officially declared emergency makes travel to campus infeasible.

USC Department of Public Safety - UPC: (213) 740-6000, HSC: (323) 442-120 – 24/7 on call
dps.usc.edu
Non-emergency assistance or information.

Office of the Ombuds - (213) 821-9556 (UPC) / (323-442-0382 (HSC)
ombuds.usc.edu
A safe and confidential place to share your USC-related issues with a University Ombuds who will work with you to explore options or paths to manage your concern.

*Occupational Therapy Faculty Practice - (323) 442-33*40 or otfp@med.usc.edu
chan.usc.edu/otfp
Confidential Lifestyle Redesign services for USC students to support health promoting habits and routines that enhance quality of life and academic performance.