Course Title: Quantum aspects of cryptography

Faculty Name: Atul Singh Arora

Name of the Program: Computer Science Elective (UG3/UG4/Dual degree)

Course Code: New course

Credits : 4

Semester, Year: Winter/Spring 2025

Pre-Requisites: Mathematical maturity from courses like Discrete Structures or Linear Algebra.

Desirable: Familiarity with the basics of (classical) cryptography, and quantum computation/information

Course Outcomes: The primary goal of this course is to enable students to perform research in this exciting newly emerging discipline. The students will be able to do the following:

CO.1 (Understand level) — Demonstrate familiarity with the basic security definitions in the area, including those of verification of quantum computations, homomorphic computation, including those based on complexity theoretic assumptions such as the hardness of the learning with errors problems.

CO.2 (Analyse) — Analyse whether a formal security definition is meaningfully capturing the relevant notion of security, and construct security proofs given explicit candidate constructions or show impossibility given a model of computation.

CO.3 (Evaluate level) — Review the literature at the frontier of quantum cryptography and related areas.

CO.4 (Evaluate level) — Evaluate the runtime/resource requirements of cryptographic protocols, derive reductions to show protocols satisfy appropriate security definitions.

Course Topics:
Depending on the maturity of the students, the course will be adapted. The following is an ambitious and therefore tentative course outline. The basic goal will be to cover Unit 1 and one key result from Units 2, 3 and 4. The remaining units will be covered, depending on the pace of the course and interest of the students.

Unit 1: Review:

Primer on quantum formalism. [VW ’16]

Lay of the land:

Impagliazzo’s worlds: in particular MiniCrypt and Cryptomania
Introduce the main directions:

(T1) post-quantum cryptography
(make classical constructions secure against quantum adversaries),
(T2) quantum analogues of classical functionalities,
(T3) functionalities impossible without quantum (excluding those in T2),
(T4) basing cryptography on quantum complexity

(T3) Information Theoretic: key distribution (BB84, Ekert), proof of security, secret sharing, impossibility of bit commitment, impossibility of strong coin flipping, achieving optimal strong coin flipping using weak coin flipping, self-testing CHSH, all bipartite states can be self-tested [VW ’24]

Unit 2: (T2) Verification:
- Regev’s quantum reduction [Regev’09]
- Weak quantum verifier: based on MBQC [GKK17]
- Classical verifier: assuming LWE is hard, Mahadev [Mahadev 18, Vidick 22]
- Classical verifier: two non-communicating provers [RUV 12]

Unit 3: (T2) QFHE: construction and its applications:
- Mahadev’s QFHE construction [Mahadev 17]
- Compiling non-local games [KLVY 23]
- Verification assuming QFHE [NZ 23]

Unit 4: (T4) Minimal assumptions: Minicrypt and below
- OT is in Miniqcrypt [GLSV 20, BCKM 20]
- Crypto despite having NP=P or similar [Kre 21, KQST 23]
- Microcrypt Primitive Zoo [Or Sattah]

Unit 5: (T1/T2) Multi Party Computation
- (T1) Post-quantum Commitments (collapse-binding commitments) [Unruh’16]
- (T1) Post-quantum MPC [HSS 11]
- (T2) Quantum 2-PC [DNS ’10 and ‘12]
- (T2) Quantum MPC w/ quantum communication [Dulek, Grilo, Jeffery, Majenz, Schaffner]
- (T2) Quantum MPC w/ classical communication [Bartusek ‘21]

Unit 6: (T3) Quantum-only functionalities—I
- Unclonable encryption: construction in the Random Oracle Model [AKLLZ ‘22]
- Certified deletion [BK ’22]
- Quantum Pseudorandom unitaries [MH ‘24]

Unit 7: (T3) Quantum-only functionalities—II
- Quantum Money and Lightning [Zhandry ‘17]
- iO for pseudo-deterministic functions [BKNY ‘23]

Unit 8: Bonus/extra reading (references will be provided later)

Other key topics in cryptography:
- Interactive proofs
- Zero knowledge
- Quantum rewinding
- Quantum Random Oracle Model
- Everlasting security

Connections to physics:
- Self-testing using a single quantum device
- Non-locality => Proof of quantumness + rigidity
- Black hole radiation decoding and commitments
- Cryptographic tests of python’s lunch conjecture
- Computationally bounded theory of entanglement

References:

GKK 17: Verification of quantum computation: An overview of existing approaches
VW 24: Introduction to Quantum Cryptography (book)
VW 16: Quantum Proofs (survey)
RUV 12: Classical command of quantum systems
Vidick 22: Course FSMP, Fall'20: Interactions with Quantum Devices
Mahadev 18: Classical verification of quantum computations
Mahadev 17: Classical Homomorphic Encryption for Quantum Circuits
KLVY 23: Quantum Advantage from Any Non-Local Game
NZ 23: Bounding the Quantum Value of Compiled Nonlocal Games: From CHSH to BQP verification
BCKM: One-Way Functions imply Secure Computation in a Quantum World
MH24: How to Construct Random Unitaries
Or Sattah: MicroCrypt Zoo
Kre21: Quantum pseudorandomness and classical complexity
KQST21: Quantum cryptography in algorithmica
DNS '10: Secure two-party quantum evaluation of unitaries against specious adversaries
DNS '12: Actively Secure Two-Party Evaluation of any Quantum Operation
DGJMS '19: Secure Multi-party Quantum Computation with a dishonest majority
Bartusek '21: Secure Quantum Computation with Classical Communication
BK 22: Cryptography with Certified Deletion
HSS11: Classical Cryptographic Protocols in a Quantum World
Unruh'16: Collapse-binding quantum commitments w/o random oracles
AKLLZ '22: On the Feasibility of Unclonable Encryption and more
Zhandry '17: Quantum Lightning Never Strikes the same state twice
MH '24: How to Construct Random Unitaries
BKNY '23: Obfuscation of pseudo-deterministic quantum circuits
Regev '09: On Lattices, Learning with Errors, Random Linear Codes, and Cryptography

Video Tutorials:

Dakshita Khurana: Cryptography with certified deletion
Mark Zhandry: Security Reductions (multi-part series)

Preferred/reference Textbooks:

There are no textbooks for this course as the material is at the frontier of current research in quantum cryptography. Relevant lecture notes/tutorials/survey articles have already been referenced above.

Resources to review basics of quantum info/computation

- Lecture notes on Quantum Computation by John Preskill (Caltech)
- Introduction to Quantum Information and Computation, MA Nielsen and IL Chuang

Resources to review classical cryptography

- Introduction to Modern Cryptography. Jonathan Katz and Yehuda Lindell.
- Foundations of Cryptography (Volumes 1 and 2). Oded Goldreich.

Other resources

- Zhandry's lecture notes on quantum cryptography

Grading Plan:

Type of Evaluation	Weight (%)
Assignments/Scribe	40
Term Paper	20
Two Exams (mid-semester and final)	40 (20 + 20)

Assignments. Approximately, every two lectures. Will largely consist of completing proofs that could not be carried out in class. Resources will be provided for finding the proofs. Deadlines for assignments will be decided by consensus. Every student is allowed to miss the deadline by at most 48 hours, at most once per month.

Exams. The final exam would not overlap (to the extent reasonable) with the material assessed in the mid-semester exam. Two previously assessed assignments can be resubmitted, one during the mid-term and one during the final, to improve one's score on those assignments. Depending on the need, one may also offer to scribe a lecture, to improve one's score on one of the assignments.

Term Paper.
The goal here is for each student to read and understand a related paper. To this end, the course requires each student to submit a short four-page summary of the paper (page limit is not strict) that also identifies one potential direction for further research, together with some ideas on how to make progress towards achieving it. The research aspect does not have to be anything too ambitious. The emphasis will be on understanding the main result. Depending on the number of students, there may be a presentation in addition/instead of the written report.
The choice of paper must be finalised before the mid-term. A list will be provided but students are welcome to submit papers they find interesting.
The term paper will be due at least one month after the mid-term. The exact date will be announced after the mid-term.

For Office Use Only
(starts on a new page)

Mapping of Course Outcomes to Program Objectives: (1 – Lowest, 2—Medium, 3 – Highest, or a '-' dash mark if not at all relevant). Program outcomes are posted at

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3	PSO4
CO1	2	2	2	1	1	1	-	-	2	2	1	2	3	2	3	3
CO2	2	2	3	1	2	-	-	-	2	2	1	2	3	2	3	3
CO3	2	2	3	1	1	-	-	-	2	2	1	2	3	2	3	3
CO4	2	2	3	1	1	1	-	-	2	2	2	1	3	2	3	3

Teaching-Learning Strategies in brief (4-5 sentences):

The course will facilitate inter-student and faculty student interactions by periodic gaps for completing in-class exercises and discussing their solutions. Proofs will be broken down into smaller steps and some steps will be given as exercises after each class. Spaced repetition of exercises will be used to encourage retention of key ideas and concepts. The focus will primarily be on understanding and asking questions, preparing the students to conduct research. The course explicitly has an exploratory component that will allow students to study cutting edge research papers and formulate new research directions and crystalise ideas on how to make progress along these directions. Students will submit written reports and, time permitting, also present their work. Both being crucial skills for conducting effective research.