TEXAS A&M UNIVERSITY

SYLLABUS

Course title and number	CSCE 689: foundations of post-quantum cryptography
Term (e.g., Fall 200X)	Fall 2018
Meeting times and location	TBD

Course Description and Prerequisites

The advance of quantum computing offers unprecedented speedup for solving fundamental problems in many disciplines. In the meantime, however, it also brings in devastating threats to cryptography, which forms a pillar of the existing cybersecurity infrastructure. Efficient quantum algorithms can break popular public-key cryptography (e.g., RSA). Unique quantum capabilities and the puzzling nature of quantum information make it extremely challenging to model and analyze cryptographic constructions in the presence of quantum attacks.

In this course, we will identify broadly three categories of quantum attacks: 1. related to quantum superposition; 2. related to quantum side information; and 3. related to quantum entanglement. We will then concentrate on the first two categories and take case studies of various cryptographic primitives to develop techniques to cope with these quantum attacks in a formal framework. Later in the course, as part of the course project, students (individually or in small groups) will prepare lectures and lead discussions on extended topics on securing classical cryptography against quantum attacks.

There is no official prerequisite for this course. You need to be comfortable with math (linear algebra and probability theory in particular), reading and writing mathematical proofs, and analysis of algorithms and basic complexity theory (NP-Completeness etc.). Prior knowledge in cryptography and quantum computing is helpful but not required. We will introduce the essence of the quantum computing, as well as necessary materials in cryptography as we go along. This course is graduate-level and upper-division undergraduates may take it upon permission of the instructor.

Note: this course will establish a formal foundation for research in post-quantum cryptography, which aims to design classical schemes (i.e., implementable on classical computers) secure against quantum attacks. We do not discuss the specific proposals but rather focusing on developing the framework and toolkit for provable quantum security. This also stands in contrast to quantum cryptography, which designs quantum protocols (i.e., quantum technology is needed to implement them) for cryptographic goals. All this can be dubbed quantum-safe cryptography.

Learning Outcomes or Course Objectives

Upon completion of this course, students will be able to:

- Understand and identify possible threats of quantum attacks on conventional cryptography.
- Apply basic quantum algorithms to attack existing cryptosystems.
- Analyze and prove security of some cryptosystems against quantum attacks using techniques related to quantum query complexity and quantum information theory.
- Critically read and present research papers.

Instructor Information

Name	Fang Song
Telephone number	TBD
Email address	TBD
Office hours	TBD

Office location TBD

Textbook and/or Resource Material

No text required. Research papers and lecture notes will be assigned throughout the semester.

Grading Policies

Homework: 40%. 2 assignments. Late homework is accepted, subject to penalty of 20% (<1 day), 40% (1-2 days), 60% (2 – 3 days), and 100% (> 3days).

Project: 40%. In-class presentation (25%) and final report (15%).

Participation: 10%.

Scribe note: 10%. Each student will be expected to scribe a subset of lecture notes.

Grading Scale: A = 90-100 B = 80-89 C = 70-79 D = 60-69 F = <60

Course Topics, Calendar of Activities, Major Assignment Dates

Week	Topic	Required Reading
1 – 3	Intro. Quantum computing basics; Simon's algorithm and Grover's quantum search algorithm	Watrous lecture notes
4 – 5	Case study: pseudorandom functions and permutations. Quantum superposition attacks on symmetric key primitives; quantum polynomial method; quantum oracle indistinguishability	Katz lecture note, Zhandry'FOCS12, Childs lecture note, Kaplan et al.'Crypto16
6 – 7	Case study: hash functions. Security against quantum generic attacks; iterated hash design	Yuen'QIC14, Zhandry'QIC15, HRS'PKC16
8 – 9	Case study: random oracle model. program a quantum random oracle; quantum security of Full-Domain-Hash signature	Unruh'JACM15, ES'TQC15,Zhandry'Crypto12
10 – 11	Case study: zero-knowledge proofs. Challenges with quantum side information; quantum rewinding; quantum proofs of knowledge;	Katz lecture note, Watrous'SICOMP09, Unruh'Eurocrypt12, HSS'Crypto11
12 – 14	Extended topics and project presentations	Quantum-secure message authentication, quantum-secure two-party computation, quantum commitment, entanglement-assisted attacks, quantum adversary method, etc.

Americans with Disabilities Act (ADA)

The Americans with Disabilities Act (ADA) is a federal anti-discrimination statute that provides comprehensive civil rights protection for persons with disabilities. Among other things, this legislation requires that all students with disabilities be guaranteed a learning environment that provides for reasonable accommodation of their disabilities. If you believe you have a disability requiring an accommodation, please contact Disability Services, currently located in the Disability Services building at the Student Services at White Creek complex on west campus or call 979-845-1637. For additional information, visit http://disability.tamu.edu.

Academic Integrity

For additional information please visit: http://aggiehonor.tamu.edu

"An Aggie does not lie, cheat, or steal, or tolerate those who do."

Collaboration on homework problems is highly encouraged, but you must write up solutions entirely on your own and clearly indicate who you worked with for each problem.