QUANTUM ALGORITHMS AND CRYPTOGRAPHY

PROF. SHWETA AGRAWAL
Department of Computer Science and Engineering
IIT Madras

PRE-REQUISITES : Theory of Computation, Design and Analysis of Algorithms, Foundations of Cryptography

COURSE OUTLINE :

The course will cover the exciting impact on cryptography created by the advent of quantum computers. Quantum computers, which harness the power of quantum mechanics, have demonstrated surprising power over classical computers -- in particular, a famous algorithm by Shor demonstrates that most of modern cryptography, believed to be secure against classical computers, is completely insecure against quantum computers. Moreover, significant progress has been made in recent times to develop quantum computers (for instance, Google recently announced that it can demonstrate "quantum supremacy"), so it is an urgent need to base cryptography on problems that remain hard against quantum attackers.In this course, we will study the foundations of quantum computing and the important role of quantum computers in cryptography. We will study the basics of quantum computing, speedups offered by quantum algorithms, attacks on cryptography using quantum computers, design of cryptosystems resilient to quantum attacks and (if time allows) cryptographic protocols using quantum physics, such as quantum key distribution, quantum money, and more.

ABOUT INSTRUCTOR :

Prof. Shweta Agrawal is an associate professor at the Computer Science and Engineering department, at the Indian Institute of Technology, Madras. She earned her PhD at the University of Texas at Austin, and did her postdoctoral work at the University of California, Los Angeles. Her area of research is cryptography and information security, with a focus on post quantum cryptography. She has won multiple awards and honours such as the Swarnajayanti award, best paper award at Eurocrypt, invited speaker at prestigious conferences like Asiacrypt, Latincrypt and “Women in Mathematics” and program co-chair for the flagship conference Asiacrypt.

COURSE PLAN :

Week 1: Mathematical Model for Quantum Mechanics, Single and multi-qubit quantum gates and circuits
Week 2: Entanglement, No Cloning, Quantum Parallelism.
Week 3: Quantum Algorithms: Deutsch-Jozsa, Simons, Bernstein-Vazirani,
Week 4: Quantum Foruier Transform, Grover's Algorithm, Shor's Algorithm
Week 5: Quantum Foruier Transform, Grover's Algorithm, Shor's Algorithm
Week 6: Useful Lattice Problems. Learning with Errors and Short Integer Solution problem. Connection to dihedral hidden subgroup problem.
Week 7: Basic Primitives. Post quantum public key encryption, signatures.
Week 8: Quantum Hardness of Lattice Problems
Week 9: Quantum key distribution
Week 10: Quantum oblivious transfer
Week 11: Quantum Random Oracles
Week 12: Quantum Money