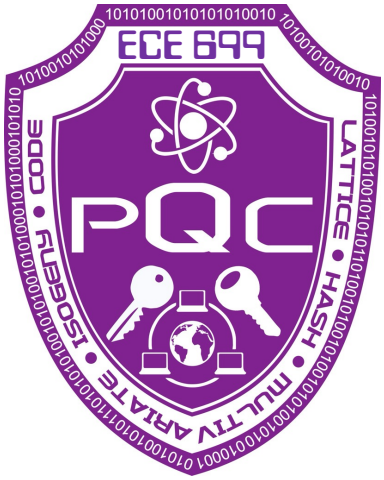

ECE 699-001/DL1
Post-Quantum Cryptography

Prerequisites: Any course on fundamentals of cryptography, including online courses

What is it about?

Cryptography that is

- resistant to all known attacks using both classical and quantum computers
- capable of being implemented using traditional software and hardware (no quantum technology required! plug-and-play solution!)

Why this course is worth taking?

- The biggest revolution in cryptography since the invention of public-key cryptography almost 50 years ago
- Emerging national and international standards
- 10-year obligatory migration to post-quantum cryptography (PQC) in the U.S. National Security Systems (NSS); commercial sector likely to follow!
- Planned inclusion in all major Internet security protocols
- Excellent job prospects and start-up opportunities

What will you learn?

- How is PQC different from traditional public-key cryptography, such as RSA, in terms of basic operations, key sizes, performance
- How to graphically visualize and fully understand basic operations without deep knowledge of math
- How to efficiently implement PQC algorithms in software and hardware
- How to make implementations resistant to side-channel attacks, such as timing, power, and electromagnetic analysis
- How to effectively incorporate PQC into existing Internet protocols
- How to effectively migrate from classical to post-quantum cryptography