ECE 395/495 Secure Quantum Computing

Prof. Jakub Szefer

This seminar course covers the emergent field of Secure Quantum Computing (SQC). Through book and research paper readings and discussion, this course will introduce students to the critical concerns of security and privacy arising from execution of quantum circuits on untrusted and often remote quantum computing servers. The course will provide introduction to relevant security and quantum computing topics, then cover topics of physical and remote attacks, side-channels and fault injection, and other potential vulnerabilities in the hardware, architecture, or software of quantum computers. The course will build a foundation for students to develop security-critical thinking and work on designing and implementing defenses for quantum computers. Students are expected to participate in active reading of the books chapters and papers, discussions and presentations. Extended homework or quarter-long project will be part of the course.