COMPUTER SCIENCE & ENGINEERING
UNIVERSITY OF MICHIGAN

DISSERTATION DEFENSE

Zack Pepin

Algebraic Structure in Lattice Cryptography

Tuesday, June 17, 2025
9:00am – 11:00am
3725 Beyster / Hybrid – Zoom

ABSTRACT: Lattice-based cryptography, i.e., the study of cryptographic schemes whose security is based on the presumed hardness of conjectured hard problems on lattices, has become an increasingly popular area of research since the seminal work by Ajtai. Later, Regev introduced the Learning With Errors (LWE) problem, which now serves as the basis for countless cryptographic constructions. Since then, many have improved upon these cryptographic constructions by introducing additional algebraic structure to the lattices, such as Ring-LWE, Module-LWE, and Middle-Product-LWE. This additional structure can be utilized in multiple ways: lattices and matrices can be more compactly represented, and more efficient algorithms exist for computing on them. However, this additional structure has the potential to weaken the conjectured hardness of structured LWE or the underlying ideal lattice problems, since we are no longer considering problems over general (unstructured) lattices, but strict subsets of these lattices.

We improve upon this situation in two main ways:

- We construct a new generalized LWE variant, which captures all the previously known algebraically structured LWE variants as special cases, as well as a new modular collection of tight reductions between various instantiations. We then use these new tools to present two new hardness results for Middle-Product LWE and Module-LWE via reductions from Ring-LWE.
- Utilize this algebraic structure, in perhaps less obvious ways, to improve the efficiency of fully-homomorphic encryption.

CHAIR: Prof. Chris Peikert