COMPUTER SCIENCE & ENGINEERING
UNIVERSITY OF MICHIGAN

DISSERTATION DEFENSE

NAVID ALAMATI

Algebraic Frameworks for Cryptographic Primitives

Friday, November 6, 2020
3:00 pm
Virtual

ABSTRACT: A fundamental goal in theoretical cryptography is to identify the conceptually simplest abstractions that generically imply a collection of other cryptographic primitives. For symmetric-key primitives, this goal has been accomplished by showing that one-way functions are necessary and sufficient to realize primitives ranging from symmetric-key encryption to digital signatures. By contrast, for asymmetric primitives, we have no (known) unifying simple abstraction even for a few of its most basic objects. Moreover, even for public-key encryption (PKE) alone, we have no unifying abstraction that all known constructions follow. The fact that almost all known PKE constructions exploit some algebraic structure suggests considering abstractions that have some basic algebraic properties, irrespective of their concrete instantiation.

We make progress on the aforementioned fundamental goal by identifying simple and useful cryptographic abstractions and showing that they imply a variety of asymmetric primitives. Our general approach is to augment symmetric abstractions with algebraic structure that turns out to be sufficient for PKE and much more, thus yielding a “bridge” between symmetric and asymmetric primitives. We introduce two algebraic frameworks that capture almost all concrete instantiations of (asymmetric) cryptographic primitives, and we also demonstrate their applicability by showing their cryptographic implications. Therefore, rather than manually building different cryptosystems from a new assumption, one only needs to build one (or more) of our simple structured primitives, and a whole host of cryptosystems immediately follows.

CHAIR: Prof. Chris Peikert