The McMicken College of Arts & Sciences
Department of Mathematical Sciences presents a

Candidate's Colloquium

Dr. Seungki Kim

Postdoctoral Research Fellow
Korea Institute of Advanced Study

Thursday, February 23, 2017
4 – 5 pm
Rm 240 WCharlton Hall

A study of a lattice reduction algorithm

The celebrated LLL algorithm by the two Lenstra brothers and Lovasz, despite its ubiquity in computational mathematics and central position in lattice-based cryptography, has never been given a serious inspection on its behavior. In particular, it has been well known since the inception of the algorithm in 1982 that its average output quality is significantly better than the guaranteed worst-case bound; this is an important phenomenon to try to understand for many reasons e.g. making accurate security estimates, yet it still remains a folklore mystery to this day. I'll discuss a series of recent works by myself and other collaborators aimed at answering this question. Thanks to the insights of A. Venkatesh and J. Ding, among others, we now have not only a much clearer picture of this phenomenon, but also a plausible potential explanation as to why it happens. Our research draws from numerous branches of mathematics, from the state-of-art algorithmic implementations to the very abstract theory of automorphic forms.
The talk is made accessible to the general mathematical audience.

Refreshments will be served 3:15 - 3:45 pm in the
Faculty & Graduate Student Lounge
Room 4118 French Hall West

UNIVERSITY OF Cincinnati