1163-68-724 **Shi Bai***, Florida Atlantic University, 777 Glades Road, Boca Raton, FL 33431. *Concrete hardness in lattice-based cryptography.*

The learning with errors (LWE) problem introduced by Regev (STOC'05) is one of the fundamental problems in lattice-based cryptography. It has been used extensively as a security foundation, for public-key encryption, signatures, fully homomorphic encryption, pseudo-random functions and many others.

A lattice-based strategy to solve the LWE problem often reduces the LWE problem to a unique SVP (uSVP) problem via Kannan's embedding and then applies a lattice reduction to solve the underlying uSVP problem. In this talk, we will discuss and compare several lattice-based strategies for solving LWE, and give some concrete estimates for breaking variants of LWE. Furthermore, we will discuss some recent developments in lattice reduction algorithms and discuss refined concrete hardness analysis. (Received September 11, 2020)