Abstract

The Learning with Errors (LWE) problem has been proven to be a versatile basis for building various purpose post-quantum schemes. In this talk, we will report our study on the hardness of the Entropic Module-LWE problem. Adapting the “lossiness approach” to the module setting, we give lower entropy bounds for the secret distribution which guarantees the hardness of Module-LWE. We will also discuss some applications of our result. This is a joint work with Hao Lin, Yang Wang, and Mingqiang Wang.