Combinatorial methods for solving LWE

Thomas Johansson

This talk gives an overview of combinatorial algorithms for solving the learning with errors (LWE) problem. We will discuss various problem instances of interest and overview the BKW algorithm. We present various improvements to BKW, including lazy modulus switching and coded-BKW. We will also present some recent improvements using a combination of sieving in lattices and coded-BKW.