Abstract

Many lattice-based crypstosystems employ ideal lattices for high efficiency. However, the additional algebraic structure of ideal lattices usually makes us worry about the security, and it is widely believed that the algebraic structure will help us solve the hard problems in ideal lattices more efficiently. In this talk, we present some interesting phenomenon about the additional algebraic structure of ideal lattices.