Abstract

The shortest vector problem (SVP) over ideal lattices is closely related to the Ring-LWE problem, which is widely used to build post-quantum cryptosystems. Power-of-two cyclotomic fields are frequently adopted to instantiate Ring-LWE. Pan et al. explored the SVP over ideal lattices via the decomposition fields and, in particular determined the length of the shortest vector in prime ideals lying over rational primes $p \equiv 3, 5 \pmod 8$ in power-of-two cyclotomic fields. In this talk, we precisely characterize the length of the shortest vector in prime ideals over rational primes $p \equiv 7, 9 \pmod{16}$ under canonical embedding. Furthermore, we derive a new upper bound, which is tighter than the Minkowski bound. Our key technique is to investigate whether a generator of a principal ideal can achieve the shortest length after embedding as a vector.