Abstract

NTRUEncrypt is generally recognized as one of candidate encryption schemes for post quantum cryptography, due to its moderate key sizes, remarkable performance and potential capacity of resistance to quantum computers. However, the previous provably secure NTRUschemes are only based on prime-power cyclotomic rings. Whether there are provably secure NTRUschemes over more general algebraic number fields is still an open problem. In this work, we present new provably secure NTRUschemes over any cyclotomic field. The security of our scheme is reduced to a variant of learning with errors over rings (Ring-LWE). More precisely, the security of our schemes are based on the worst-case approximate shortest independent vectors problem over ideal lattices.