Abstract

Based on hardness of ideal syndrome decoding problem, we propose a new IND-CPA-secure NTRU-like KEMs under rank metric. We give the parameter sets and make comparison with some NIST candidates.