# Abstract

Based on hardness of the rank support learning problem which is as hard as the rank syndrome problem, we introduce a new IND-CPA-secure public-key encryption scheme--Loong-1.CPAPKE. By applying a variant of the Fujisaki-Okamoto transform to Loong-1.CPAPKE, a new IND-CCA-secure key encapsulation mechanism (KEM for short) Loong-1.CCAKEM can be constructed. Based on the same difficult problem, we also propose a new IND-CPA-secure KEM, i.e., Loong-2.CPAKEM. Finally, we make comparison on parameter sets between our schemes and some NIST submissions.