Abstract

Cloud storage and computing offers significant convenience and management efficiency in the information era. Privacy protection is a major challenge in cloud computing. Public key encryption with keyword search (PEKS) is an ingenious tool for ensuring both privacy and functionality in certain scenario, such as ensuring privacy for data retrieval appearing in the cloud computing. Despite many attentions received, PEKS schemes still face several challenges in practical applications, such as low computational efficiency, high end-to-end delay, vulnerability to inside keyword guessing attacks. In this talk, we will discuss efficient PEKS constructions based on RLWE.