ORAL DEFENCE ANNOUNCEMENT

LI ZHE

Post Quantum Cryptographic Constructions

With the past and ongoing developments of quantum computers, the existing asymmetric schemes are no longer secure. Thus, we need to actively find quantum resistant cryptographic constructions. To date, there are many proposals based on different hard mathematical problems. This thesis seeks to enrich the diversity of the quantum resistant schemes and improve the efficiency of existing schemes. We present constructions from coding theory, lattices and subset sum problems.

Date: 4 December 2020
Time: 1 PM
Supervisor: Prof Ling San
Co-Supervisor: Prof Xing Chaoping