ORAL DEFENCE ANNOUNCEMENT

ZHANG JUANYANG

Revocable cryptosystem from lattices

Lattices have become one of the most powerful tools in constructing cryptographic schemes. For a multi-user cryptosystem, revocation has been a necessary but challenging problem. The PhD topic is to investigate revocation model and the associated lattice-based instantiations. A series of cryptosystems supporting efficient revocation are constructed, such as server-aided revocable identity-based encryption and predicate encryption schemes and directly revocable predicate encryption scheme.

Date: 23 May 2018
Time: 3PM
Venue: Conference Room, Research & Graduate Studies Office, Level 2, SPMS
Supervisor: Assoc Prof Wang Huaxiong