Lattices in Constructions of Dense Sphere Packings and Certain Cryptographic Schemes

In this thesis, we provide some instances, especially in sphere packing and cryptography, to demonstrate the potential of lattices in multi-disciplinary research.

First we introduce special concatenating methods using codes and lattices from number fields to construct dense sphere packings in Euclidean spaces. Next we develop the recent techniques in lattice-based cryptography to construct a policy-based signature scheme from lattices. Our construction can be extended to a delegatable policy-based signature, thanks to the hierarchical structure of the Bonsai tree. Finally we present a revocable identity-based encryption scheme from lattices by combining two Agrawal et al.’s identity-based encryption schemes (Eurocrypt 2010) with the subset difference method. In particular, our scheme may serve as a solution to a question posed by Chen et al. (ACISP 2012).

Date: 28 March 2016 (Monday)
Time: 2pm
Venue: NTU SPMS MAS Executive Classroom 1, SPMS-MAS-03-06
Supervisor: Prof Ling San
Co-Supervisor: Prof Xing Chaoping