ALGORITHMS AND ESTIMATES FOR LATTICE-BASED CRYPTOGRAPHY

Speaker: 白石教授

上海交通大学

Time: Mon, Jun 1st, 13:00 - 14:00
Venue: 光华东主楼 1801

Abstract:

量子计算的迅速发展对传统密码体系构成潜在威胁，也推动了抗量子密码的研究。格密码作为后量子密码的重要分支，其安全性基于格上困难问题的计算复杂性。错误学习问题（Learning with Errors, LWE）是格密码的核心基础问题。本报告将聚焦于 LWE 问题的量子算法求解，系统介绍当前主量子攻击算法及其计算复杂度估计，并对其量子算法的复杂性进行评估和比较。