摘要

该报告简要介绍了高维格密码体制设计与分析的几个基本科学问题，包括：对格密码分析与安全性评估密切相关的格基约化算法 LLL 和格的最短向量问题（SVP）求解算法；格密码体制所基于的困难问题的归约化证明；格密码体制的陷门单向函数的设计方法，特别是高斯采样算法。