摘　要

本报告给出一种基于密码群作用的通用承诺方案构造框架。该框架基于密码群作用的自归约特性，设计了重随机化算法与随机性提取器组件，并证明其可以自然导出基础承诺方案的构造，并扩展至 Dual-Mode 等高级承诺方案的构造。我们首次基于格同构问题（LIP）与格自同构问题（LAP）实现该框架。