摘要

本报告将从代数的角度介绍几种密码分析方法，探讨其代数性质及其变种，包括数值映射理论、相关立方攻击、差分线性分析等，以及它们在著名密码算法分析中的应用，内容涵盖了我们近年来在 CRYPTO 密码学年会和 EUROCRYPT 密码学年会上发表的最新研究成果。