中邑 聡史 (九州大学大学院数理学府 修士課程)

【講演概要】:

現在広く使われている RSA 暗号や楕円曲線暗号は量子計算機によって容易に解読されることが示されている．それに対し，格子暗号は耐量子性を持つ次世代暗号として期待されている．本講演では、格子暗号の安全性を支える Shortest Vector Problem (SVP)の求解アルゴリズムの改良とその開発について発表する.