共同利用

情報セキュリティ基盤の数理構造と安全性解析

種別	短期共同研究
研究計画題目	情報セキュリティ基盤の数理構造と安全性解析
研究代表者	前野　俊昭（京都大学大学院　工学研究科・講師）
研究実施期間	平成24年9月3日（月）～ 平成24年9月7日（金）
研究分野のキーワード	情報セキュリティ、ハッシュ関数、擬似乱数生成器、量子情報、安全性解析、離散数理、最適化
目的と期待される成果	多様な情報セキュリティ基盤の理論的安全性評価に向けて、それらに共通する数理構造を抽出・整理し定量的な安全性解析の一般的な枠組を定式化することが目的である。特に、従来定量的な安全性評価の難しかった対象や、量子情報などの新しいトピックを中心に扱うことで、次世代情報技術の理論的基礎に対して広く適用可能な数理的手法の確立を目指すと共に、離散数理として興味深い新しい問題を発掘し幅広い観点からの研究を行う。そのために情報セキュリティの研究者と数学者からなる研究チームを組織し、最新の研究動向の報告、問題意識の共有のための議論を行う。具体的な成果としては、ハッシュ関数や擬似乱数、暗号などに対する定量的安全性評価方法の提案と共に、基礎となる数学的問題や、関連して現れる新しい数理構造に関する理解を深めることを目指している。関係の深い発展的テーマとして、量子情報理論の枠組での解析や電子透かし、認証技術等への応用に関する話題も視野に入れて研究を進める。
組織委員(研究集会) **参加者(短期共同利用)**	阿部　拓郎（京都大学・講師） 伊豆　哲也（富士通研究所・主任研究員） 鍛冶　静雄（山口大学・講師） 木村　元（芝浦工業大学・助教） 鈴木　幸太郎（NTT情報流通プラットフォーム研究所・主任研究員） 仲田　研登（稚内北星学園大学・講師） 縫田　光司（産業技術総合研究所・研究員） 沼田　泰英（東京大学/JST CREST・特任研究員） 栗原　大武（京都大学数理解析研究所・GCOE特定研究員）