共同利用

高機能暗号とプライバシー保護情報分析の基盤数理

種別	短期共同研究
研究計画題目	高機能暗号とプライバシー保護情報分析の基盤数理
研究代表者	縫田　光司（産業技術総合研究所　情報技術研究部門・主任研究員）
研究実施期間	平成28年9月5日（月）～ 平成28年9月8日（木）
研究分野のキーワード	暗号技術、高機能暗号、プライバシー保護情報分析、表現論、組合せ論
目的と期待される成果	消費者の行動履歴の分析に基づく物流・物販の最適化や、患者の遺伝情報の分析に基づく創薬・医療技術の発展など、プライバシーに関わる情報の分析への産業的な期待が高まっている。同時に、人々のプライバシーを適切に保護しつつ情報分析を行うための暗号技術も重要性を増している。プライバシー保護情報分析で主要な役割を果たす暗号技術は、情報秘匿や認証など単純な機能に留まらず、例えばデータを暗号化したままで計算するなどの高度な機能を実現する。それらは比較的新しい暗号技術であり、その安全かつ効率的な実用化を支える理論的基盤が充分に整備されているとは言い難い。その整備の遅れの一因として、それら高機能暗号が基盤とする数学の高度化・複雑化傾向が挙げられる。しかしこのことは逆に、数学者の立場からそうした暗号分野の課題解決に取り組む価値と必要性の高さを示唆している。本応募の短期共同研究では、産業界における暗号・プライバシー保護技術の研究者と、代数学、幾何学、組合せ論など複数分野の数学者が集まり、産業的観点で重要な当該分野の喫緊の数学的研究課題の解決を目指すとともに、当該分野の今後の中長期的発展の方向性を見据え、その際に必要性が見込まれる基盤数学理論の開拓にいち早く取り組む。
組織委員(研究集会) 参加者(短期共同利用)	縫田　光司（産業技術総合研究所 情報技術研究部門 高機能暗号研究グループ・主任研究員） 阿部　拓郎（京都大学・講師） 鍛冶　静雄（山口大学・講師） 栗原　大武（北九州工業高等専門学校・講師） 沼田　泰英（信州大学・准教授） 前野　俊昭（名城大学・准教授） 野﨑　隆之（山口大学・助教）
成果報告書	【Web公開】成果報告書_共20160015.pdf