共同利用

代数的手法による数理暗号解析に関する研究集会

種別	一般研究_研究集会(II)
研究計画題目	代数的手法による数理暗号解析に関する研究集会
研究代表者	高島克幸（三菱電機 情報技術総合研究所 松井暗号プロジェクトG・主席技師長）
研究実施期間	平成30年2月5日（月）～ 平成30年2月7日（水）
研究分野のキーワード	代数幾何、代数的組み合わせ論、楕円曲線暗号、ペアリング暗号、格子暗号
目的と期待される成果	【目的】高度かつ急速に進化する現代の情報社会において、情報セキュリティを支える暗号は現代生活において必須の技術となっている。現在広く普及している公開鍵暗号としてRSA暗号と楕円曲線暗号が最も代表的であり、これらの暗号技術の安全性はそれぞれ素因数分解問題と楕円曲線離散対数問題と呼ばれる数学問題の計算量困難性に基づいている。さらに、高機能性かつ耐量子性の両方を備えた次世代暗号である格子暗号の安全性は最短ベクトル探索問題などの格子問題の計算量困難性に基づいている。このように、現代暗号技術は楕円曲線や格子理論など主に代数学関連の数学分野と非常に深い関係にある。本研究集会では、代数学と暗号の研究者間の積極的な交流を促すことを目的とする。より具体的には、双方が持つ各分野における高度な専門知識・最新情報を共有すると共に、互いの研究課題に対して他分野からのアプローチを試みることで、既存研究では得られなかった新しい研究の方向性を探索することを目的とする。 【期待される成果】本研究集会において、代数学と暗号の研究者間の積極的な交流を通して、各研究分野における既存アプローチには得られなかった新しい研究の方向性を生み出すことが期待できる。更には、複数の研究分野にまたがったシナジー効果が期待でき、長期的・永続的な研究交流を促進することが期待できる。
組織委員(研究集会) 参加者(短期共同利用)	安田雅哉（九州大学マス・フォア・インダストリ研究所・准教授） 縫田光司（産業技術総合研究所・主任研究員） 阿部拓郎（九州大学マス・フォア・インダストリ研究所・准教授）
成果報告書	【Web公開】成果報告書_共20170015.pdf