共同利用

理論・計算数学と暗号学の融合アプローチによる次世代暗号構築の新展開

種別	若手研究_短期共同研究
研究計画題目	理論・計算数学と暗号学の融合アプローチによる次世代暗号構築の新展開
研究代表者	工藤桃成（神戸市立工業高等専門学校・講師）
研究実施期間	令和2年2月3日（月）～ 令和2年2月7日（金）
研究分野のキーワード	計算代数・数式処理，格子理論，多変数暗号，ポスト量子暗号
目的と期待される成果	本研究の目的は，既存および次世代の暗号方式について，理論数学・計算数学・暗号学が三位一体となって安全性評価を行い，産業界との連携を強化しながら，将来的により実用的で頑強な暗号通信の実現に貢献することである．さらに，最新の数学理論と計算技術の融合的知見に基づく暗号方式を新たに提案することも目指す． 現在普及している暗号方式であるRSA暗号と楕円曲線暗号は，それぞれ素因数分解問題と楕円曲線離散対数問題という数学問題の計算困難性に安全性の根拠を置いている．しかしながら，量子計算機の大規模化が進行すると，これらの数学問題は現実的な時間で求解されるため，RSA暗号や楕円曲線暗号は安全ではなくなることが知られている．このため近年では，米国国立標準技術研究所（NIST）が耐量子計算機暗号の公募を行うなど，量子計算機に耐性のある暗号方式およびその安全性根拠となる数学問題の研究・提案が産官学を巻き込んで活発になされている． 本研究では，耐量子と考えられている既存の数学問題に加え，新しいタイプの数学問題を提案し，理論数学・計算数学・暗号学の先進研究を結集・融合させることで，これら三方向からの安全性評価を十分に行い，耐量子性の数学問題として最適かつ実用的なものを選定し，安全な暗号パラメータの算出を行う．具体的には、以下の事柄を扱う． (i) 様々なグレブナー基底計算アルゴリズムを用いた多変数暗号の安全性評価 (ii) 格子基底簡約アルゴリズムの実験的，理論的計算量評価の解析 (iii) 代数幾何，計算機代数などを組み合わせた新しいタイプの数学問題の構成と評価 本研究により，これまで異なる方向から独立になされてきた安全性評価研究の融合・一体化を行い，産業界の需要を取り込むことで，既存研究より高い信頼性と実用性を兼ね備える耐量子暗号の実現が期待できる．そしてそれらの研究に伴い，実験結果も含めた新たな耐量子暗号研究に関する有用な知見を得ることもできる. また，暗号方式の実装や解読において使用される個々のアルゴリズムの改良や，新たなアルゴリズムの提案などによって，理論数学や計算数学における様々な問題を解決するための新たなツールを提供することが可能となる．
組織委員(研究集会) 参加者(短期共同利用)	池松泰彦（九州大学マス・フォア・インダストリ研究所・助教） 高安敦（東京大学大学院情報理工学系研究科数理情報学専攻・助教） 中村周平（日本大学生産工学部教養・基礎科学系・助手） 坂田康亮（横浜国立大学大学院環境情報学府・大学院生） 工藤桃成（神戸市立工業高等専門学校・講師） 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主管技師長） 深作亮也（九州大学大学院数理学研究院・助教）