# 研究課題別事後評価結果

１．研究課題名：　次世代暗号に向けたセキュリティ危殆化回避数理モデリング

２．研究代表者名及び主たる研究参加者名（研究機関名・職名は研究参加期間終了時点）

研究代表者

高木　剛（東京大学大学院情報理工学系研究科　教授）

主たる共同研究者

若山　正人（東京理科大学データサイエンスセンター　客員教授）

田中　圭介（東京工業大学情報理工学院　教授）

國廣　昇　（筑波大学システム情報系　教授）

３．事後評価結果

〇評点：

| |
|---|
| A+　非常に優れている |

〇総合評価コメント

４つの研究グループがそれぞれの特徴を生かし、暗号の安全性を保証するモデリングの研究を行ってきた。様々な数学問題の解答手続きの長大さをもとに暗号が組み立てられている現在、その解答を高速に求める方法が暗号への攻撃となる。研究期間の前半で現在定式化されている格子暗号に対し、数理的に高速解法を導き、計算量評価を行うとともに、そのアルゴリズムを用いて暗号解読コンテストで世界記録を達成した。また、現在使われている RSA 暗号等に対する安全性評価を行うとともに、量子計算機が実用化された後にも有効な暗号技術の開発に関して、理論面で基礎的な量子模型やラマヌジャングラフの検討をおこない、企業との共同研究による実用的な成果も得ている。これらの研究成果は、学術論文(275 編)、書籍(15 件)、暗号国際会議を含む発表(486 件)により、研究者に公開している。また社会を支える暗号理論として社会的関心の高い分野であるが、数学が安全性を支える鍵であることがわかる研究成果として、一般向けにもなる図書やマスコミを通じて広報されている。社会への貢献として特筆すべきは、将来の社会の基礎を形成するポスト量子暗号の標準化 NIST とのかかわりである。まず暗号方式を提案したが、それは採択には至らなかった。その後、評価者として参画を続けており、NIST で採択された方式において計算量が小さく暗号が脆弱となる場合の発見などで貢献し高く評価されている。延長研究期間においても、それを実装していくうえで重要な効率的な署名方式を代数における剰余環の理論を用いて導き提案している。また、新しい同種写像暗号方式の提案を行っている。今後も、様々な暗号の安全性評価のための理論を含めた研究、様々な数学問題の困難性評価などとともに、新しい暗号方式の開発も視野に入れた研究を推進していくことが十分に期待できる。これに関して、研究課題の遂行の中でチームとして多くの若手研究者を育てており、今後の研究を支えるものとなっている。