# 研究課題別中間評価結果

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：　高木　剛　（九州大学マス・フォア・インダストリ研究所　教授）

３．中間評価結果

研究代表者のもと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いる。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。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ている。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うとともに、実際的に提案されてくる様々なポスト量子暗号の標準化にも参画している。これらの研究成果は、国際的に高く評価されており、学術雑誌および書籍により公開されている。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、マスコミを通じて広報されていることは重要である。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ただきたい。