研究課題別事後評価結果

１．研究課題名：　楕円曲線を用いた耐量子計算機暗号の安全性解析と高効率化

２．個人研究者名

相川　勇輔（三菱電機（株）情報技術総合研究所　研究員）

３．事後評価結果

耐量子計算機暗号の候補として有力な同種写像暗号について、理論および実装の両方面からの研究を行った。同種写像暗号は楕円曲線に関する大量の演算を必要とする方式のため効率性に課題があった。本研究では同種写像暗号で用いられる KLPT アルゴリズムと構成的 Deering 対応アルゴリズムの改良に取り組み、従来より高速な実装を得た。また、楕円曲線の種々の演算を統一的に扱うために一般化モンゴメリー座標を導入し、楕円曲線の演算の計算効率性を扱う理論的フレームワークを整備した。さらに、他の ACT-X 研究者とともに超特別アーベル多様体の同種写像グラフのスペクトラルギャップの理論解析を行った。耐量子計算機暗号に関連した話題についての招待講演を複数回行っており、研究成果を社会に還元する活動にも積極的に取り組んだ。ACT-X の他の研究者との交流も積極的に行った。このように、同種写像暗号について理論・実装の両面において精力的に研究を進めており、今後もさらなる進展が期待できる。