「イノベーション創発に資する人工知能基盤技術の創出と統合化」
平成 28 年度採択研究代表者

H28 年度
実績報告書

花岡　悟一郎

国立研究開発法人産業技術総合研究所情報技術研究部門
研究グループ長

安全な秘匿化データ処理を実現する汎用依頼計算技術

§1. 研究実施体制

(1)暗号理論設計グループ
① 研究代表者:花岡　悟一郎 （国立研究開発法人産業技術総合研究所　情報技術研究部門、研究グループ長）
② 研究項目
・汎用秘匿化依頼計算アルゴリズムの理論設計

(2)応用分野実装グループ
① 主たる共同研究者:浅井　潔 （国立大学法人東京大学大学院　新領域創成科学研究科メディカル情報生命専攻、教授）
② 研究項目
・汎用秘匿化依頼計算技術に基づくアプリケーションとビジネスモデルの開発

§2. 研究実施の概要

本研究においては、入出力情報を秘密に保ったままデータ処理を高速に実行する汎用のプラットフォームを構築し、情報漏えいの心配のない多様なアプリケーションを社会に実装可能とする、**汎用秘匿化依頼計算技術**（図 1）の実現を目的としている。初年度にあたる平成 28 年度においては、関連する要素技術と応用技術について研究動向調査を行い、それを踏まえ、暗号理論設計グループにおいて秘匿化データ処理の理論設計の対象とする計算クラスの初期選定を、応用分野実装グループにおいて実装の対象とする秘匿化ゲノムデータ処理の選定をそれぞれ進めている。

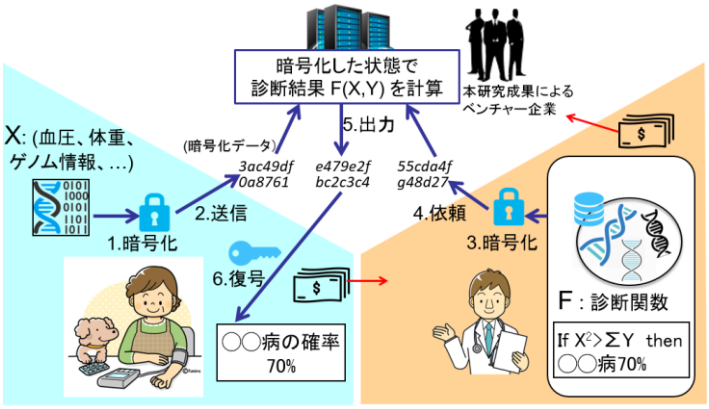

図 1 汎用秘匿化依頼計算システムの概観

【暗号理論設計グループ】

要素技術に関する研究動向調査を行い、暗号要素技術（関数暗号、Multi-Party Computation、準同型暗号など）および、それらを用いた秘匿化データ処理に関する最新の知見を得ている。また、安全で効率的な関数暗号の構成方法を自ら考案し、その性能評価を行った。具体的には、安全で効率的な関数暗号の実現方法についての検討を行い、特に、適応的安全性と呼ばれる関数暗号において考えられる最高レベルの安全性の一般的な達成方法を明らかにした[1]。さらに、応用分野実装グループによる下記の検討結果をもとに、秘匿化の対象とするデータ処理の計算クラスの初期選定を進め、実装を行うデータ処理の候補の絞り込みを行った。

[1] Nuttapong Attrapadung, Dual System Framework in Multilinear Settings and Applications to Fully Secure (Compact) ABE for Unbounded-Size Circuits, Proc. of PKC 2017 (Part II), Lecture Notes in Computer Science 10175, pp.3-35, 2017.

【応用分野実装グループ】

応用分野において、基盤的な秘匿計算応用技術と、アプリケーションを開発する対象について、研究動向調査と検討を行った。特に、秘匿計算応用技術に関する研究動向調査として、秘匿化計算理論から実装システムへ変換するためのコンパイラとプログラミングフレームワークやゲノムデータ処理等の応用に関するケーススタディについて調査を行った。これにより、生命情報工学分野において通常想定されるデータ処理の秘匿化に必要な要素技術が明らかとなり、その知見を暗号理論設計グループに入力することで、本研究において秘匿化の対象とするデータ処理の計算クラスの初期選定に貢献した。