「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

H29 年度
実績報告書

花岡悟一郎

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 (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 (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。平成 29 年度においては、前年度に引き続き、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処理システムの初期設計と要素技術の洗練化を、応用分野実装グループにおいてアプリケーションの開発と汎用秘匿化依頼計算技術に求められるシステム要件の洗い出しをそれぞれ進めている。

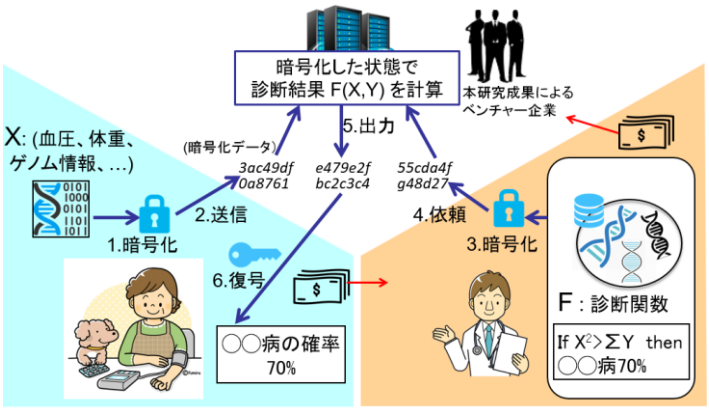

図 1 汎用秘匿化依頼計算システムの概観

【暗号理論設計グループ】

前年度から平成 29 年度初めまでに行った研究動向調査に基づいて要素技術の選定を行い、秘匿化処理システムの初期設計を行った。また、その基盤となる理論的フレーワークの構築を進め、さらに、要素技術となるツールセットの洗練化も行っている。本年度開発された要素技術の例として、耐量子性をもつ効率的な ID ベース暗号[1]等が挙げられる。本年度開発を行った初期設計システムはすでに高度な汎用性を備えており、いくつかのアプリケーションを容易に構成できただけでなく、実用に耐えうる処理速度が得られている。

[1] S. Yamada, Asymptotically compact adaptively secure lattice IBEs and verifiable random functions via generalized partitioning techniques, Proc. of CRYPTO 2017, Vol. 10403 of LNCS, pp. 161-193, Springer, 2017.

【応用分野実装グループ】

これまで、加法準同型暗号を中心に応用アプリケーションを開発して来たが、より広範囲の対象に秘匿計算を適用するための基本的なツールとして、任意の回数の加法に加えて1回の乗算を暗号空間で行うことができ、かつ効率的な暗号を開発して実装した[2]。具体的な応用としては、秘匿文字列検索を準同型暗号と Wavelet Matrix を用いて高速に行う手法を開発して実装し、有効性を検証した[3]。また、差分プライバシとマルチパーティ計算を組み合わせて、薬剤感受性予測の性能を向上させることに成功した。

さらに、より社会実装に近い応用アプリケーションとして、SNS 会話から秘匿計算によって最も広告価値の高い広告を表示するデモを、レベル2準同型暗号を用いて作成した。

[2] N. Attrapadung et al., Efficient two-level homomorphic encryption in prime-order bilinear groups and a fast implementation in WebAssembly, Proc. of ASIACCS 2018, to appear.

[3] H. Sudo et al., Secure Wavelet Matrix: Alphabet-friendly privacy-preserving string search for bioinformatics, IEEE/ACM Transactions on Computational Biology and Bioinformatics, presented in GIW2017 and accepted for publication in TCBB, 2018.