社会変革に向けた ICT 基盤強化　　2022 年度
2022 年度採択研究代表者　　年次報告書

藤木 大地

慶應義塾大学 理工学部
助教（テニュアトラック）

メモリ駆動形 DB システムによるデータ処理基盤強化

研究成果の概要

メモリ中心型計算とデータベース処理の親和性を高めるための Processing-in-Memory（PIM）の要素技術について、PIM とコンピューティングシステムの協調動作に関連する課題を解決することにより、その大幅な拡張を行った。PIM によってデータ構造の様々な見方を変える、ビューと呼ばれる用法を定義し、その入力および出力に関する局所性の活用法が未発見であったため、その方法論の検討を行った。また、従来の方法での一貫性の保証が性能のオーバーヘッドとなっていることを明らかにした。ビューを認識するキャッシュコヒーレンスプロトコルの拡張を導入することで、入力の一貫性のマネジメントの簡素化、および、出力の一貫性・再利用性の活用を、既存のコヒーレンスプロトコルに則る形で可能となることを示した。キャッシュコヒーレンスプロトコルの拡張は、モデルバリデーションツールを使用した Formal Verification により、その動作を確認した。さらに、提案手法が、行保存型インメモリデータベースでの解析処理といった比較的簡単なアクセスパターンをもつワークロードから、連結リストなどランダムなアクセスパターンをもつデータ構造まで様々な最適化ができるという知見を得た。

また、効率的な秘密計算データベースの実現のため、3 者間でのマルチパーティー計算による秘密情報取得（PIR）や 2 者間での準同形暗号による PIR 手法を検討し、その課題点を明らかにした。特に 3 者間での PIR では、秘密分散の手法に従えばクラウドにランダムシャッフルされた情報へのアクセスログしか残らないため、この特性を活用することで全件検索を前提とせずともアクセスに関する情報が秘匿化できることを示した。また、回転可能な準同形暗号をもちいることで、特殊な制約なしで信頼のおけないクラウドを使用した PIR が実現できるという知見を得た。