社会変革に向けた ICT 基盤強化　　2022 年度
2021 年度採択研究代表者　　年次報告書

照屋 唯紀

産業技術総合研究所 情報・人間工学領域
主任研究員

プライバシ保護メカニズムデザインのための秘密計算技術

研究成果の概要

秘密計算の実行は高コストであり、効率的なプロトコルの開発は本研究において重要な研究課題である。高速化のアプローチの一つとして、多くの計算を一括りにしてこれを並列に実行する方法が考えられる。しかし、通常の秘密計算技術は個々のデータの値は秘匿できるが、どのデータがどの計算の入出力かという、個々の計算に対する所属情報を秘匿できない。このような並列化による秘匿性の問題は、例えば、グラフ構造に対する最短経路探索やデータベース処理において Group By 処理を用いる場合などに生じ得る。

本研究ではこの問題を解決する安全かつ高速な並列秘密計算プロトコルを提案した [1]。この秘密計算プロトコルは、半群を成す二項演算を計算する秘密計算プロトコルをビルディングブロックに用いて、この二項演算によって Scan (Prefix Sum)計算として記述できる複数の計算を一括して並列に計算することができ、さらに、どのデータがどの Scan 計算に所属するかという所属情報を秘匿できる。既存プロトコルに対し、提案プロトコルは計算に必要なビルディングブロックの実行回数が少なく、その結果として高速かつ通信量が少ない安全な並列秘密計算プロトコルの実現が可能である。上で述べたように、この提案プロトコルが適用可能となる条件は、ビルディングブロックとなる秘密計算プロトコルが計算する演算が半群を成すことであり、メカニズムデザインの分野に限らず様々な分野に応用できる。取り扱うアルゴリズムが用いる演算がこの条件に合致し、上で述べた並列化によって生じる秘匿性の問題の解決が必要な場合には、この提案プロトコルを適用することで、安全にそのアルゴリズムの計算を高速化することが期待できる。

【代表的な原著論文情報】

1) “Secure Parallel Computation on Privately Partitioned Data and Applications”, Proceedings of ACM CCS 2022, pp.151-164, 2022