基礎理論とシステム基盤技術の融合による Society 5.0 のための基盤ソフトウェアの創出　　2022 年度年次報告書

2022 年度採択研究代表者

アッタラパドゥン ナッタポン

産業技術総合研究所 サイバーフィジカルセキュリティ研究センター
研究チーム長

サステナブルな分散型秘密計算基盤

主たる共同研究者:

川村 信一（産業技術総合研究所 サイバーフィジカルセキュリティ研究センター 研究チーム長）
松浦 幹太（東京大学 生産技術研究所 教授）
松田 隆宏（産業技術総合研究所 サイバーフィジカルセキュリティ研究センター 研究チーム長）
米山 一樹（茨城大学 大学院理工学研究科工学野 教授）

研究成果の概要

秘密計算は、データを秘匿したまま処理が可能な暗号技術であり、個人・企業の機密情報の利活用を促進すると期待されている。本研究は、「秘密計算プロバイダへの信頼の必要性」及び「プロバイダが不在の状況の運用の困難性」の課題を解決し、分散環境下の効率的な秘密計算の基礎理論確立、及び、ユーザインセンティブ設計が組み込まれ持続可能な運用が可能となる基盤開発を行い、サステナブルな分散型秘密計算基盤を目指す。本年度は、主に以下の成果が得られた。

- 秘密計算において、並列処理は計算の効率化だけでなく、データ構造や制御構造を秘匿するためにも本質的である。本研究においては、様々な計算クラスに対応可能な「秘密並列計算」の最適なプロトコルを提案した [1)]。提案方式は、通信回数を（入力長に対して）対数的、秘匿演算回数を最適（理論下限に一致）とする初めてのプロトコルであり、従来方式と比べ 50% 以上の通信量削減を可能とした。
- ビットコインなどの暗号通貨で攻撃者に金銭的ペナルティを科す仕組みを構築することで、公平な秘密計算を実現できる。本提案基盤の目的の一つである公平性の実現に向けて、金銭的ペナルティに基づく公平な秘密計算において、通信ラウンド数の改善手法を新たに提案した [2)]。従来手法では通信ラウンド数がパーティ数に比例して増加する課題があったが、提案手法ではこれを参加者数に依存しない定数に改善した。

【代表的な原著論文情報】

1) Nuttapong Attrapadung, Hiraku Morita, Kazuma Ohara, Jacob C. N. Schuldt, Tadanori Teruya, Kazunari Tozawa: Secure Parallel Computation on Privately Partitioned Data and Applications. ACM CCS 2022: 151-164
2) Takeshi Nakai, Kazumasa Shinagawa: Constant-Round Linear-Broadcast Secure Computation with Penalties. Theoretical Computer Science, 2023 (to appear)