2023 年度年次報告書
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、個人や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」および「プロバイダが不在の状況の運用の困難性」という課題を解決し、分散環境下での効率的な秘密計算の基礎理論を確立することを目指している。また、ユーザインセンティブ設計が組み込まれた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の構築を目指している。

本年度は、主に以下のような成果を得た。まず、効率的な秘密計算に関して、様々な計算を含むクラスの秘密計算における通信のボトルネック複雑性を低減する手法を提案し、これを国際会議 ASIACRYPT 2023 で発表した。また、秘密計算とゼロ知識証明を応用し、検証可能かつプライバシーが保護される機械学習プロトコルを提案し、国際会議 ACNS 2024 で発表した。

さらに、公平な秘密計算を実現するために金銭的ペナルティを科す仕組みを構築した。この研究は、金銭的ペナルティに基づく公平な秘密計算において効率的な方式を提案し、その成果は国際論文誌 Theoretical Computer Science に掲載された。また、信頼できる銀行による法的な強制力を導入することで公平性を保証する秘密計算方式については、従来は 2 者間に限定されていたが、我々は初めて多者間方式を実現し、これを国際会議 ICICS 2023 で発表した。

【代表的な原著論文情報】

1) Reo Eriguchi: Unconditionally Secure Multiparty Computation for Symmetric Functions with Low Bottleneck Complexity. ASIACRYPT (1) 2023: 335-368
2) Nuttapong Attrapadung, Goichiro Hanaoka, Ryo Hiromasa, Yoshihiro Koseki, Takahiro Matsuda, Yutaro Nishida, Yusuke Sakai, Jacob C. N. Schuldt, Satoshi Yasuda: Privacy-Preserving Verifiable CNNs. ACNS (2) 2024: 373-402
3) Takeshi Nakai and Kazumasa Shinagawa, "Constant-Round Linear-Broadcast Secure Computation with Penalties" Theoretical Computer Science, vol. 959, Elsevier, 2023.
4) Takeshi Nakai and Kazumasa Shinagawa, "Secure Multi-party Computation with Legally-Enforceable Fairness" 25th International Conference on Information and Communications Security (ICICS 2023), LNCS, vol. 14252, Springer, 2023.