2024 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を行う暗号技術であり、個人や企業の機密情報の安全な利活用を可能にする手段として注目されている。本研究は、「秘密計算プロバイダへの信頼の必要性」や「プロバイダ不在時の運用の困難性」といった課題を解決し、分散環境における効率的かつ持続可能な秘密計算基盤の構築を目指している。

本年度は、効率性・安全性・公平性の観点から多くの成果を挙げた。効率化では、状態を保持したまま並列処理を行う新たな秘密計算モデルを提案し、通信量を大幅に削減できるプロトコルを設計した（ACM CCS 2024）。安全性では、任意クエリに対応可能な能動的セキュリティを備えた秘匿検索手法を開発した（EUROCRYPT 2024）。また、秘密計算における報酬配分の公平性確保に向けたプロトコル設計とその実装にも取り組んだ。

さらに、分散性の高いアクセス制御を実現するため、マスター秘密鍵を不要とする登録型属性ベース暗号の構成を提案し、柔軟かつ拡張性に富む設計を実現した（CRYPTO 2024）。そのほか、秘匿決定木評価の通信効率化（PoPETs 2024）、Ethereum 2.0 に関連するブロックチェーンのコンセンサス機構に対して脆弱性対策と高速化の両立を図る新技術の提案（ACSAC 2024／WEB3SEC）なども行い、秘密計算の応用展開と基盤技術の高度化に向けた重要な進展を達成した。

【代表的な原著論文情報】

1) Nuttapong Attrapadung , Kota Isayama , Kunihiko Sadakane , Kazunari Tozawa. Secure Parallel Computation with Oblivious State Transitions. ACM CCS 2024: 3008-3022
2) Reo Eriguchi, Kaoru Kurosawa, Koji Nuida. Efficient and Generic Methods to Achieve Active Security in Private Information Retrieval and More Advanced Database Search. EUROCRYPT (5) 2024: 92-121
3) Nuttapong Attrapadung, Junichi Tomida. A Modular Approach to Registered ABE for Unbounded Predicates. CRYPTO (3) 2024: 280-316
4) Nan Cheng, Naman Gupta, Aikaterini Mitrokotsa, Hiraku Morita, Kazunari Tozawa. Constant-Round Private Decision Tree Evaluation for Secret Shared Data. Proc. Priv. Enhancing Technol. (PoPETS) 2024(1): 397-412 (2024)
5) Shinsaku Naito, Kanta Matsuura. Fast and Secure Consensus Protocol for Ethereum 2.0. ACSAC Workshops 2024 (WEB3SEC): 280-287