AIP 加速課題　　2022 年度

2022 年度採択研究代表者　　年次報告書

花岡 悟一郎

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
首席研究員

秘匿計算による安全な組織間データ連携技術の社会実装

主たる共同研究者:

盛合 志帆（情報通信研究機構 サイバーセキュリティ研究所 研究所長）
小澤 誠一（神戸大学 数理・データサイエンスセンター 教授）
菅原 貴弘（(株)エルテス 代表取締役）

研究成果の概要

本課題初年度となる 2022 年度においては、先行して実施した CREST 課題での成果に基づき、X 社および Y 技術組合から抽出した具体的なシステム要件を反映することで、これら企業・機関における実システム上で即稼働可能な技術の開発を進めた。また、協力銀行にシステム導入したプライバシー保護連合学習の持続的・長期的な運用に向け、判定結果の継続的な検証及び新たなデータによる継続的な追加学習とその効果について検証を行った。

花岡グループでは、特に、効率的な秘匿逆行列および秘匿べき乗計算アルゴリズムを設計し、それらに基づいて秘匿逆行列計算説明変数の秘匿化も可能な秘匿ベイズ最適化アルゴリズムの構成を行った。盛合グループでは、小澤グループと連携し、協力銀行にシステム導入したプライバシー保護連合学習の持続的・長期的な運用に向け、顧客口座データの標準化と疑わしい取引に関する判定基準の標準化を進めた。小澤グループでは、判定結果の継続的な検証及び新たなデータによる継続的な追加学習とその効果について研究・検証を行った。具体的には、LightGBM などで使われている Gradient-based One-Side Sampling を改良し、継続学習の下で希少正例データを優先的に残しながら、過去の負例データの多様性を維持するサンプリング手法を提案した。菅原グループでは、CREST 時に実証実験を行っていた被害口座検知に加えて、新たに加害口座検知システムの導入と連合学習の本格的な試験導入支援を行った。

【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,” Proc. ACM-CCS 2022, pp.151-164, 2022.
2) Sachiko Kanamori, Taeko Abe, Takuma Ito, Keita Emura, Lihua Wang, Shuntaro Yamamoto, Le Trieu Phong, Kaien Abe, Sangwook Kim, Ryo Nojima, Seiichi Ozawa, Shiho Moriai: Privacy-Preserving Federated Learning for Detecting Fraudulent Financial Transactions in Japanese Banks. Journal of Information Processing. 30: 789-795 (2022)
3) Septiviana Savitri Asrori, Lihua Wang, Seiichi Ozawa: Permissioned Blockchain-Based XGBoost for Multi Banks Fraud Detection. ICONIP 2022: 683-692
4) Nuttapong Attrapadung, 花岡 悟一郎, 松田 隆宏, 大原 一真, 照屋 唯紀, “秘密計算によるベイズ最適化” CSS 2022 予稿集, 2022.