Society5.0 を支える革新的コンピューティング技術
2019 年度採択研究代表者

2021 年度
年次報告書

本間尚文

東北大学　電気通信研究所
教授

耐量子計算機性秘匿計算に基づくセキュア情報処理基盤

§1. 研究成果の概要

本年度は，5 項目の研究開発項目について，下記の研究成果を得た．

(1) 耐量子計算機性準同型暗号に基づく汎用秘匿情報処理技術

耐量子計算機暗号に基づく確率的秘匿演算アルゴリズムの効率化を推進するとともに，その秘匿推論処理への応用により，その有効性を定量的に示した．さらに，耐量子計算機性暗号のハードウェアアルゴリズムを開発し，従来を上回る性能見積りを得た．

(2) 物理攻撃に対して頑健なセキュアシステム実装技術

測定性能を高めたセキュア秘匿計算プラットフォームのコアとなる評価ボードを開発した．また，開発したボードをコアとした実験環境下において，耐量子計算機準同型暗号への物理攻撃評価の高精度化および秘密情報漏えいを設計時に評価可能なシミュレーションセットアップを構築した．

(3) 秘匿推論コンピューティング技術

これまでに進めてきた決定木構造の情報リークを防いだ推論プロトコルについて，BGV，TFHE の 2 種類の暗号を用いて性能評価を行った．決定木構造の情報リークを防ぐことで，Path Finding Attack と呼ばれるモデル抽出攻撃に必要な推論回数を最大 5 倍程度増加させることを確認した．さらに，機械学習モデル種別も秘匿可能な秘匿推論方式の検討を開始した．

(4) 秘匿プロセッシング技術

トーラス型完全準同型暗号を用いてデータおよびプログラムの暗号化・復号処理を実行するための基本ライブラリを構築し，NAND を含む複数の 2 入力論理関数の評価を可能とした．また，より大規模な論理関数を効率よく評価するための実行エンジンを作成した．さらに，仮想プロセッサの構成と仮想プロセッサがサポートする命令セットを定義し，概念実証のためのプロトタイプを構築した．

(5) 耐量子・耐タンパー性秘匿計算セキュアプラットフォーム

上記技術を統合した耐量子計算機性・耐タンパー性セキュア秘匿計算プラットフォームのプロトタイプ構築に着手した．また，秘匿推論技術と秘匿プロセッシング技術の連携に着手した．

§2. 研究実施体制

(1)秘匿計算基盤グループ

① 研究代表者:本間 尚文 (東北大学電気通信研究所 教授)

② 研究項目

・耐量子計算機性秘匿計算に基づくセキュア情報処理基盤技術の開発

(2)セキュアシステム実装グループ

① 主たる共同研究者:林 優一 (奈良先端科学技術大学院大学先端科学技術研究科 教授)

② 研究項目

・物理攻撃に対して頑健なセキュアシステム実装技術の開発

(3)秘匿推論コンピューティンググループ

① 主たる共同研究者:橋本 昌宜 (京都大学大学院情報学研究科 教授)

② 研究項目

・秘匿推論コンピューティング技術の開発

(4)秘匿プロセッシンググループ

① 主たる共同研究者:佐藤 高史 (京都大学大学院情報学研究科 教授)

② 研究項目

・秘匿プロセッシング技術の開発

【代表的な原著論文情報】

1) "Imbalanced Data Problems in Deep Learning-Based Side-Channel Attacks: Analysis and Solution," IEEE Transactions on Information Forensics and Security, Vol.16, pp. 3790-3802, June 2021
2) "Virtual Secure Platform: A Five-Stage Pipeline Processor over TFHE," in Proc. USENIX Security Symposium, pp.4007-4024, August 2021.
3) "Curse of Re-encryption: A Generic Power/EM Analysis on Post-Quantum KEMs," IACR Transactions on Cryptographic Hardware and Embedded Systems, Vol. 2022, Issue 1, pp. 296-322, DOI:10.46586/tches.v2022.i1.296-322, November 2021.
4) "Bypassing Isolated Execution on RISC-V using Side-Channel-Assisted Fault-Injection and Its Countermeasure," IACR Transactions on Cryptographic Hardware and Embedded Systems, Vol. 2022, Issue 1, pp. 28-68, DOI:10.46586/tches.v2022.i1.28-68, November 2021.
5) "Fault-Injection Attacks against NIST's Post-Quantum Cryptography Round 3 KEM Candidates," International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT2021), pp.33-61, DOI:10.1007/978-3-030-92075-3_2,

December 2021.