Society 5.0 を支える革新的コンピューティング技術　　2022 年度
2019 年度採択研究代表者　　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

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）
橋本 昌宜（京都大学 大学院情報学研究科 教授）
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）

## 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開発を推進し，多項式関数や推論処理への応用により有効性を定量的に示した．特に，その耐量子計算機性暗号化・復号ハードウェアアクセラレータを開発し，従来の秘匿演算アルゴリズムと比較して 2 桁の性能向上を達成した．

(2) 物理攻撃に対して頑健なセキュアシステム実装技術

開発するセキュア秘匿計算プラットフォームのコアとなる耐量子計算機性暗号 HW 設計・評価ボードの第 3 版を開発した．また，開発したボードをコアとした実験環境下において，電磁的な情報漏えいをシステム設計時に評価可能なシミュレーションモデルを構築した．

(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推論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．さまざまな推論処理に適用した結果，入力ビット数が小さい場合は BGV，大きい場合は TFHE が有効であることを明らかにした．さらに，機械学習モデル種別も秘匿可能な秘匿推論方式を引き続き検討した．

(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主要要素技術（コンパイラ，命令セット，TFHE 実行エンジン，CPU/GPU 向け TFHE ライブラリ）の開発を完了し，AWS およびさくらインターネットによる商用クラウドを用いて動作実証および性能評価を行った．結果，従来比 1600 倍の高速化を達成することを明らかにした．

(5) 耐量子・耐タンパー性セキュア秘匿計算プラットフォーム

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を構築した．また，秘匿プロセッシングの主要要素技術を開発し，OSS ライブラリとして公開し，秘匿推論技術への適用を推進した．

【代表的な原著論文情報】


1) “On the Success Rate of Side-Channel Attacks on Masked Implementations: Information-Theoretical Bounds and Their Practical Usage,” The 29th ACM Conference on Computer and Communications Security (CCS 2022), pp.1521–1535, November 2022.
2) “Homomorphic Encryption for Stochastic Computing,” Journal of Cryptographic Engineering (2022), https://doi.org/10.1007/s13389-022-00299-6, September 2022,
3) “SASIMI: Evaluation Board for EM Information Leakage from Large Scale Cryptographic Circuits,” 2022 IEEE International Symposium on Electromagnetic Compatibility & Signal/Power Integrity (EMCSI), 2022, pp.299–302, August 2022.
4) “Perceived Information Revisited: New Metrics to Evaluate Success Rate of Side-Channel Attacks,” IACR Transactions on Cryptographic Hardware and Embedded Systems, 2022(4), pp.228–254, August 2022.
5) "ELM: A Low-Latency and Scalable Memory Encryption Scheme," IEEE Transactions on Information Forensics and Security, vol. 17, pp. 2628-2643, July 2022,