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

2020 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

2020 年度は，研究項目(1)～(3)についてそれぞれ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

前年度に引き続き効率的な秘匿演算アルゴリズムの開発を推進した．前年度に調査した耐量子計算機性準同型暗号に基づく秘匿演算方式を中心に検討し，主に 2 次関数・3 次関数を対象に開発中アルゴリズムの性能を評価した．その結果から，格子暗号を用いた方式が他の暗号を用いた方式よりも優位であることを明らかにした．また，それと並行して，格子暗号で支配的な演算となる数論変換を高速に実行する HW アルゴリズムの開発を推進した．

(2)物理攻撃に対して頑健なセキュアシステム実装技術

耐量子計算機性準同型暗号へのパッシブ攻撃（時間領域，周波数領域のサイドチャネル情報を利用したサイドチャネル攻撃）を想定した物理攻撃評価環境のプロトタイプを開発した．また，物理攻撃評価環境と合わせて提供する評価ライブラリ内のサイドチャネル情報漏えいシミュレーションツールの開発に着手した．さらに，高精度な物理攻撃評価を行うためには，従来の基板設計で求められるパワーインテグリティ（PI）と電磁両立性（EMC）を満たすだけでは不十分であることを明らかにし，新たなメトリクスを与えて設計する必要があることを示した．

(3)秘匿推論コンピューティング技術

前年度に提案した決定木向けの秘匿推論プロトコルの改良と性能分析を行った．データオーナーにパスコストが漏れることで決定木構造の推測が容易になる問題に対して，新たに乱数をかけてローテーションを行うことで，データオーナーにパスコストが漏れないプロトコルに拡張した．提案プロトコルの計算量や通信量について複雑度を分析し，アンサンブル学習を用いることで計算量や通信量を小さく抑えつつ，推論精度を向上させることが可能であることを示した．

§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 （大阪大学大学院情報科学研究科、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

【代表的な原著論文情報】

1) “ストカスティック演算を用いた確率的準同型暗号の構成に関する検討,” 電子情報通信学会情報セキュリティ研究会, Vol. 120, No. 112, ISEC2020-23, pp. 61-67, July 2020

2) “FPGA 消費電流シミュレーションに向けた要素回路に対する電気計測手法の検討,” 2021 年電子情報通信学会総合大会, A-19-3, March 2021

3) “Practical Side-Channel Based Model Extraction Attack on Tree-Based Machine Learning Algorithm,” Applied Cryptography and Network Security Workshops, LNCS 12418, pp. 93-105, October 2020

4) “Machine Learning and Hardware security: Challenges and Opportunities,” 2020 IEEE/ACM International Conference On Computer Aided Design (ICCAD), pp. 1-6, November 2020. (Invited)

5) “Diffusional Side-channel Leakage from Unrolled Lightweight Block Ciphers: A Case Study of Power Analysis on PRINCE,” IEEE Transactions on Information Forensics & Security, DOI: 10.1109/TIFS.2020.3033441, Vol.16, pp. 1351-1364, October 2020

6) “モデルとプライバシーを保護するアンサンブル決定木向け秘匿推論プロトコル,” 情報処理学会 コンピュータセキュリティシンポジウム, 1E5-4, pp. 396-403, October 2020