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

2019 年度
実績報告書

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

本研究では，超スマート社会で想定される膨大かつ多様な端末デバイスを安全にサイバー空間に接続して頑健なデータ連携・統合を実現するセキュアコンピューティング技術の確立を目指して，理論から実装までの技術レイヤーを融合した革新的セキュア情報処理基盤の研究開発を推進した．具体的には，①耐量子計算機準同型暗号に基づく汎用秘匿情報処理技術，②物理攻撃に対して頑健なセキュアシステム実装技術，および③秘匿推論コンピューティング技術の 3 項目の研究開発を推進した．

本年度は，上記 3 項目の研究開発について，それぞれ下記の研究成果を得た．

① 耐量子計算機準同型暗号に基づく汎用秘匿情報処理技術

開発対象とする耐量子計算機準同型暗号の調査を行った．特に，安全性と性能の両面で優れた特性を有する Learning With Error（LWE）問題に基づく格子暗号（LWE 暗号）を対象として，アルゴリズムの選定を進めるとともに鍵長・パラメータ等を検討した．それと並行して，有限体上のフーリエ変換（NTT）に基づく秘匿演算向け格子暗号ハードウェアアルゴリズムの開発に着手した．また，効率的な秘匿計算を実現する上での確率的数値表現を検討するとともに，それに適した暗号の仕様・方式の評価に着手した．ここでは，多様な単演算準同型暗号方式を広く候補として，新概念である確率的秘匿演算アルゴリズムの実現に適した方式を探索した．

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仕様策定に着手した．その際，サイドチャネル情報の取得・評価を容易にするための基板構造の抽出などをシンプルな評価系を用いて検討し，得られた知見を同仕様策定に利用した．

③ 秘匿推論コンピューティング技術

秘匿推論に必要な基本秘匿演算について調査を行った. 特に, ランダム/ディープ・フォレスト等の決定木を用いた機械学習アルゴリズムに着目し, その実装に適した秘匿演算方式について演算量や通信量の観点から調査・評価した. また, 評価結果に基づき, CPU 実装にてその動作を検証した. なお, 本年度の段階では耐量子計算機性にはこだわらず広く調査対象を設定した.

【代表的な原著論文】

1. 上野嶺, 本間尚文, “ストカスティック計算に基づく確率的準同型暗号の構成に関する検討,” 2020 年暗号と情報セキュリティシンポジウム (SCIS 2020), No. 1B1-1, January 2020.

§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