Graduate School of Fundamental Science and Engineering
Waseda University

博 士 論 文 審 査 報 告 書
Doctoral Dissertation Review Report

論　文　題　目
Dissertation Title

Arbitrary Function Evaluation with Fully Homomorphic Encryption Using Table Lookup

ルックアップテーブルによる準同型暗号上での任意関数の実現

申　請　者
(Applicant Name)
Ruixiao LI
李　睿筱

Department of Computer Science and Communications Engineering　Research on Parallel and Distributed Architecture

February, 2024

多種多様かつ大量のデータが社会の基盤となる Society5.0 時代において，情報漏洩，プライバシー問題の解決は喫緊の課題である．特に，近年のクラウド・コンピューティング（クラウド）の急速な利用拡大を背景として,「データ保存時だけでなく計算時を含めて，暗号のままデータを扱う」ことのできる機密性を確保した計算委託へのニーズが高まっている．本論文は，暗号化されたデータを復号せずに計算を可能とする準同型暗号（HE，Homomorphic Encryption）を用いて任意関数を実現し，情報漏洩，プライバシー問題の解決に資することを目指したものである．

本論文は，R-LWE（Ring-Learning with Errors）問題に基づく HE を用いて、任意の関数の準同形評価を構成する手法を提案している．本論文の貢献は，HE が持つ制約，すなわち HE 上では加算・乗算以外の演算を行うことができないという問題に対して，ルックアップテーブルを用いることで，機械学習で多用される ReLU 関数や Swish 関数をはじめとする任意関数を実現した点である．これにより，従来，多項式近似により実現されていた関数の精度を向上させることが可能となるだけでなく，関数実行のレイテンシを短くできる．具体的には，次の３つの貢献がある．

最初の貢献は,「３パーティモデルによる任意関数の実現」である．本モデルでは，計算委託を行うユーザ，計算サーバ（クラウド），鍵管理を行う信頼サーバを想定している．関数への入力値の分布が統計的に信頼サーバに知られることを許容することにより，短いレイテンシかつ高精度での関数実行を可能とした．ReLU 関数では，多項式近似に比較して，誤差を約 100 分の１，レイテンシを約半分にすることに成功している．本方式により，任意の 18 ビット１入力関数を 2.5 秒（４スレッドでの並列処理），任意の８ビット３入力関数を 16.9 秒（16 スレッドでの並列処理）のレイテンシで実行できることを示した．

二つ目の貢献は,「２パーティモデルによる任意関数の実現」である．本モデルでは，計算委託を行うユーザ，計算サーバ（クラウド）を想定している．鍵管理をユーザが行うことにより，データの機密性を確保している．従来の手法が２入力関数，かつ，出力データポイント数が２N（N はパッキングにより一つの暗号文に格納できる最大のデータ数（スロット数））までに制限されていたのに対し，提案手法では，任意の入力数を持つ関数を出力データポイント数に制約を設けず構築できるようにオープンエンド化を行った．15 ビット１入力関数を 4.5 秒，10 ビット２入力関数を 151.5 秒，5 ビット３入力関数を 178.3 秒（何れも 16 スレッドでの並列処理）のレイテンシで実行できることを示した．ビット単位での HE 暗号化により任意関数を構築する手法に比較すると，5 ビット３入力関数の関数において，98 倍の高速化を達成した．

三つ目の貢献は，HE を用いた実アプリケーションとして，パワーグリッドを対象に，暗号化された電力使用量に対する異常検知を実用に耐えうるレイテンシと精度で実現したことである．具体的には，３パーティモデルによる任意

関数実現方式を適用し，異常検知精度に応じて 11 秒～17 秒のレイテンシで異常検知を行うことができることを示した．

以下，各章の概要について説明する．

第 1 章は，序論である．

第 2 章は，前提知識として，本論文で用いる記号の定義，Ring-LWE 問題に基づく HE である BFV 方式，BFV 方式において適用できるパッキングと呼ばれる SIMD 計算方式，3 パーティモデルで用いる PIR（Private Information Retrieval）方式について説明している．

第 3 章は，3 パーティモデルによる任意関数の構築手法を提案している．同モデルでは，任意関数の実現に留まらず，関数への入力と出力との対応（データポイント）をルックアップテーブルに用意する際，データポイント数の制約を排除している．具体的には，関数への入力範囲全てに対してデータポイントを用意する必要性を排除し，データポイント数を任意に変更することにより，関数の精度とレイテンシを調整する手法へと拡張している．

第 4 章は，第 3 章で提案した手法の実証実験である．米国テキサス州 200 家庭の 3 年間の電力使用量データを用い，パワーグリッドを対象に，暗号化された電力使用量に対する 3 種類の攻撃に対して，実用に耐えうるレイテンシと精度で異常検知できることを示している．

第 5 章は，2 パーティモデルによる任意関数の構築手法を提案している．従来手法の制約である「関数の出力データポイント数の上限」を排除するため，ルックアップテーブル分割法を提案している．同手法では，関数への入力データを暗号文空間の小さな複数の暗号文で表現している．さらに，ルックアップテーブルを分割しマルチスレッド実行を可能とすることで関数実行のレイテンシを小さくしている．評価実験では，BFV 方式を用いた従来の手法に比較して，オープンエンドな実装となっていることを確認すると共に，ビット単位での HE 暗号化により任意関数を構築する手法に比較し，レイテンシを小さくすることができることを 1 入力から 3 入力まで，入力・出力のビット数を変えた様々な関数を実装し確認している．

第 6 章は，本論文のまとめである．

第 7 章は，本論文の結果を踏まえ，さらに研究を発展させるための展望を述べている．

以上を要するに，本論文では，Ring-LWE 問題に基づく HE を用いた任意関数の構築方法を 2 つの異なる機密性を前提として提案すると共に，実際のアプリケーション適用においても有効であることを評価している．これらの成果は，HE の実用化に大いに貢献するものであり，博士（工学）（早稲田大学）の学位論文として価値あるものと認める．

2024 年 2 月

審査員

主査	早稲田大学教授	博士（工学）（早稲田大学）	山名早人
副査	早稲田大学教授	博士（工学）（早稲田大学）	清水佳奈
副査	早稲田大学教授	博士（工学）（京都大学）	佐古和恵