博士後期課程

# 博士請求論文審査要旨

情報セキュリティ大学院大学
情報セキュリティ研究科

**論文題目**　：　A Study on Homomorphic Property of Ring-Based Lattice Cryptography
**申請者**　：　半田 沙里
**審査委員会**　：　主査　教授　有田 正剛
副査　教授　大塚 玲
副査　教授　後藤 厚宏
副査　教授　土井 洋

## Ⅰ. 論文内容の要旨

本論文は “A Study on Homomorphic Property of Ring-Based Lattice Cryptography”（環に基づく格子暗号の準同型性に関する研究）と題し、6 章からなっている。

第 1 章“Introduction”では、本論文の研究背景を述べている。データマイニングやブロックチェーンなどパブリックな環境や分散した環境でデータを計算するニーズが増えつつあり、そこでは計算エンジンに対して計算対象データの秘匿性を守りつつ計算タスクを実行することが課題となっている。そこで、データを秘匿したままで計算タスクを実行するための基盤技術である、 “Secure Computation”技術を研究対象とした旨、動機を説明している。Secure Computation 技術を計算主体が一つか複数かで分類し、一つの計算主体で計算が完結できる準同型計算に着目し、準同型計算のうち暗号スキームである準同型暗号とエンコードスキームである多重線型写像を研究対象としている。

第 2 章“Lattice-Based Cryptography”では、準同型暗号および多重線型写像の中核となる Ring-LWE 暗号を説明し、それをベースとした準同型暗号の既存研究について述べている。まず準備として格子暗号の基礎的事項および LWE 問題の定義を述べ、続いて Ring-LWE 暗号で使われる円分環に関わる代数学的事実を準備し、さらに Ring-LWE 問題の定義および Ring-LWE 暗号の構成方法を述べている。既存研究の調査では、準同型暗号の代表的な構成方法である、メッセージを上位桁に配置する FV タイプの準同型暗号方式、および下位桁に配置する BGV タイプの準同型暗号方式を説明している。

第 3 章“SIMD Operation of Homomorphic Encryption”では、準同型暗号における、並列計算の手法が説明されている。準同型暗号では、多くのスキームで、複数の平文をそれぞれ平文スロットに設定して一つの暗号文にパックし、それらパックされた暗号文同士を準同型演算することにより、複数の平文を並列に準同型処理する手法が知られている。そのような並列演算を実現する仕組みとして、中国人の剰余定理（CRT）が使われる。CRT を利用した場合の平文スロットの代数的構造は、代数体において素数がどのように素イデアルに分解するかで決まるため、素イデアル分解の様子を様々な代数体について観察している。その上で、従来の準同型暗号が用いている円分環では、各平文スロットの構造が高次元の有限体 $GF(p^d)$となり、スロットごとの整数積としての準同型性が得られるのはスロット要素を表す

有限体の要素が定数項のみからなる場合に限定されてしまうため、上記にのべた並列化手法に無駄が発生していることを指摘している。さらに、HElib、SEAL、HEAAN などの既存の準同型暗号を平文スロット構造の観点から整理し、特徴をまとめている。

第 4 章“Homomorphic Encryption Scheme Based on Decomposition Ring”では、分解環を用いた、２つの準同型暗号スキームを提案している。分解環の定義を述べ、分解環上では各スロットが整数環 $Z_p$ になることを説明し、そのため、平文スロットを用いた準同型乗算に対する、上記並列化手法の無駄を自然になくすことができ、より効率的に並列演算を実現できることを述べている。続いて分解環の基底の構成方法を明らかにした上で､分解環を用いて FV タイプと BGV タイプの準同型暗号スキーム（DR-FV および DR-BGV）を構成している。ノイズの大きさを理論的に評価することで、両スキームが共に完全準同型暗号であることを証明している。さらに、両提案スキームをソフトウェアで実装し、円分環を用いた BGV タイプの準同型暗号ライブラリ HElib と提案スキーム DR-BGV の速度比較を実施している。その結果、DR-BGV は HElib より数倍高速であるとの結果が得られ、分解環を用いることによって平文スロットを用いた並列化手法が無駄なく実行できることを実証している。安全性については、理論的な考察にもとづき、分解環をもちいた準同型暗号の安全性は円分環を用いた従来の準同型暗号と同等であるとしている。

第 5 章　“Two Applications of Multilinear Maps: Group Key Exchange and Witness Encryption”では、グレード（レベル）付きエンコードシステムとして提案された多重線型写像の応用として、グループ鍵交換と Witness 暗号を提案している。グループ鍵交換は、アップフローとダウンフローの簡単なプロトコルで、多重線型写像を利用すると一人当たりの計算コストと 1 通信あたりの通信量を参加者数によらず定数オーダーにできると述べている。また、Witness 暗号は Hamilton Cycle 問題をベースにした構成を提案している。両プロトコル共に、全パーティ（グラフの頂点）を巡って秘密を集めて積み上げ、最大レベルになった時に確定的な値を取り出すという性質を利用している。

第 6 章“Conclusions”では、分解環に基づく準同型暗号の提案と多重線形写像の応用の成果について要約し、これらによって計算対象データの秘匿性を守りつつ、より効率的に計算タスクを実行することができるとしている。

## Ⅱ. 論文審査結果の要旨

本論文は、今日の情報化社会を支える、クラウド等のパブリックな計算エンジンにおいて、データの秘匿性を守りつつデータをより高度に活用するための、具体的かつ基盤的な方法を示したものであって、情報学並びに情報社会の発展に貢献するところが大きい。よって、本論文は情報学における博士論文として十分価値のあるものと認める。

## Ⅲ. 審査経過

本審査委員会は、2019 年 7 月 25 日に論文内容について口述試問を行い、その後、2019 年 8 月 27 日これに関連する事項の最終試験審査を実施して、申請者が学位取得にふさわしい知見を持つものと判断した。

情報セキュリティ大学院大学　情報セキュリティ研究科