		指導教員	知能 花子　教授
学生番号	222C1042	氏　　名	小野 歩未
論文題目	openFHE を用いた NTRU 方式に基づく マルチキー FHE システムの構築及びその応用		

1　はじめに

昨今では様々な暗号化方式が存在するが，その中でも格子基盤暗号に分類される NTRU 方式は，計算が高速かつ量子攻撃にも耐性があるという点で優れている．また，FHE とは暗号化したデータを復号することなく直接演算を行うことができる技術であるが，異なる鍵で暗号化した複数のデータに対して演算を行うマルチキー FHE(MKFHE) を利用できるライブラリは，Go 言語で実装されている tfhe-go 等，ごく限られている．本研究では，既存のライブラリである OpenFHE を利用し，NTRU 方式に基づく MKFHE システムを構築し，またこれを利用した全加算器を実装した．

2　従来の暗号化方式と MKFHE の比較

以前より利用されてきた基本的な公開鍵暗号方式は，データを暗号化したまま演算を行っても正しい平文の結果が得られる準同型性を有していることが多い．しかしこのような従来の暗号化方式は，異なる鍵で暗号化したデータ同士の演算を想定していない．マルチキー FHE ではこれを改良し，異なる鍵で暗号化したデータ同士に演算を行っても，正しい復号結果を得ることができる．[1] このような改良によって，例えば複数のユーザそれぞれが自分の鍵ペアの公開鍵でデータを暗号化し，データの内容を誰にも明かさず集計及び演算を行えるため，セキュリティを維持しつつデータを利活用することが期待できる．

3　MKFHE の全加算器への応用

異なる鍵で暗号化したデータに加算・乗算が行えるという MKFHE の仕様は，加算器に応用することが可能である．全加算器において，考えるべき点は (1) 前の桁からの繰り上がりを考慮した現在の桁の加算，(2) 現在の桁の繰り上がりの計算，の 2 点であるが，(1) は

$$S = A \oplus B \oplus C_{in}$$

のように単純な 3 つの項の加算で表され，(2) は mod2 の世界において

$$c_{carry} = (A \oplus C_{in}) * (B * C_{in}) \oplus C_{in}$$

のように，加算と乗算を利用した式に変形することができる．以上のことから，加算器の実装には MKFHE の準同型性を利用することができる．

4　実験手法

まず，1 ビットのデータ a, b, c をランダムに設定し，加算 (排他的論理和)，乗算 (論理積)，及び 2 つを組み合わせた式をすべて暗号文の状態で正しく計算し復号できるかを確かめる．次に，これを用いて加算器を実装する．ランダムな 1〜3 ビットの長さのビット列を 2 つ生成し，正しい結果が得られたかどうかを確認する．

5　実験結果

単純な 1 ビット同士の加算・乗算を 10000 回ずつ行った際の標準偏差 σ，実行時間，復号の成功率をまとめて表 1 に示す．なお，標準偏差 σ は，NTRU 方式で MKFHE を実装する上で必要な多項式を構成する，係数の値のばらつき具合を表す．

標準偏差 σ	実行時間 [秒]	成功率
	deux	
0.35	2139.989	0.9986
0.4	183.442	0.9862

表 1: 1 ビット同士の加算・乗算処理の実行結果

また，次に実装した 1〜3 ビットの加算器についても同様の結果を以下の表 2 に示す．

標準偏差 σ	実行時間 [秒]	成功率
	deux	
eine	zwei	
0.4	183.442	0.9862

表 2: 1〜3 ビットを対象とした加算器の実行結果

6　まとめ

本研究では，既存のライブラリを用いて NTRU ベースの MKFHE による加算器を実装し，実験的なパラメータを用いて動作させることに成功した．今後の課題としては，より実用的なパラメータ下で動作させるためのアルゴリズム改良やパラメータの調節等が挙げられる．

参考文献

[1] Lopez-Alt, A., Tromer, E., & Vaikuntanathan, V. (2017). Multikey fully homomorphic encryption and applications. SIAM Journal on Computing, 46(6), 1827–1892.