		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，C++で既に実装されている openFHE というライブラリを利用し，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，RSA に代表されるような基本的な公開鍵暗号方式は，データを暗号化したまま加算や乗算を行っても正しい平文の結果が得られるという準同型性を有していることが多い．しかしながら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加算や乗算といった計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．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持つ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すことなく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

$$S = A + B + C_i n$$

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

$$c_c arry = (A + C_i n) * (B * C_i n) + C_i n$$

のように，加算と乗算を利用した式で表すことができるから，

4　注意する点

1. 基本的に通常の LaTeX と同じように利用できる．ただし，パッケージは最低限のものしか入れていないので，必要に応じて自身で `abst.tex` へ追加する．
2. 見出しは `section` と `subsection` しか使えない．
3. `baselineskip` は変更しないこと．
4. 参考文献を加える方法は，通常通りである．例えば，LaTeX の参考書には [1, 2] がある．

参考文献

[1] 野寺隆志，楽々LATEX (第 2 版)，共立出版，1994.

[2] 奥村晴彦，黒木裕介，LaTeX 2_ε 美文書作成入門 第 7 版，技術評論社，2017.