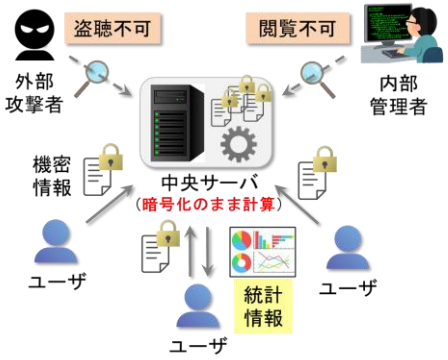
安全かつ効率的な符号ベース完全準同型暗号の構成に関する研究

A Study on the Construction of Secure and Efficient Code-Based Fully Homomorphic Encryption

潮田幹生・法制·倫理分科会・情報セキュリティ大学院大学

研究背景

量子計算機の発展に伴い，既存暗号方式の安全性が低下してしまうおそれがあるため，近年量子計算機に耐性を持つ耐量子計算機暗号(PQC)の研究開発が活発化している．PQCの方式として，格子理論を基盤とする格子暗号，誤り訂正符号理論を基盤とする符号暗号，楕円曲線の同種写像理論を基盤とする同種写像暗号等がある．
また，クラウドやビッグデータ分析の進展に伴い，機密情報の利活用とプライバシー保護の両立が課題となっており，暗号化したまま加算と乗算が可能な暗号技術である完全準同型暗号(FHE)の活用が注目されている．



準同型暗号による機密情報の利活用

研究目的

従来のFHE方式はいずれも格子暗号を基盤としたものである．本研究では，符号暗号を基盤としたFHE方式を実現し，格子ベース方式と比較した安全性や効率性に関する評価を行うことを目的とする．

先行研究

C.Aguilar-Melchor, V.Dyseryn, P.Gaborit, Somewhat Homomorphic Encryption based on Random Codes, Preprint, 2023.

ランクメトリックを利用したランダムイデアル符号のシンドローム復号問題に基づく準同型暗号方式が提案されている．しかし，乗法準同型演算を行うための再線形化処理において，公開する暗号文数がしきい値を超え，安全性が満たされないことが判明している．そのため，現時点で符号ベース準同型暗号は“完全”準同型暗号は構成されておらず，乗算に関して回数等の制限がある“somewhat”準同型暗号の構成にとどまっている．

今後の研究方針

- ランクメトリックを利用した符号暗号等の基礎知識を整理
- ガロア理論や量子計算等の周辺分野の活用を検討
- 提案方式の安全性評価と，実装による効率性を評価

2026年 1月～	4月～	7月～	10月～	2027年 1月～
基礎知識の整理	周辺分野の活用検討	方式の提案/実装･評価	追加評価/学会準備	学会発表/修論まとめ