6.6 安全なデータ利活用のための準同型暗号 PBL

[開講科目名]

(授業科目)高度セキュリティ PBL Ⅱ／(enPiT-Pro)安全なデータ利活用のための準同型暗号 PBL

[開講科目名(英)]

Advanced Security PBL Ⅱ

[単位数] 1 単位

[開講日]

(調整中)

[担当教員]

宮地 充子(大阪大学), 河内 亮周(大阪大学), 奥村 伸也(大阪大学)

[授業の目的・概要]

本科目では暗号化したまま統計処理などが可能な準同型暗号やその応用と課題を学び, 実際に実装することで習得する.

情報化社会が進むにつれ大量のデータをクラウドに預ける企業などが急激に増えてきた. さらに, クラウドサーバーはそれ自体が高い演算処理能力のあるマシンであるから, 預けたデータの統計処理等が可能であり, 様々なアプリケーションを提供することができる. しかし, クラウドデータの漏洩や信用できないクラウド管理者への対策としてデータを暗号化した状態でクラウドに預けることが望ましいが, 通常の暗号による暗号化では, 暗号化データを処理してしまうと正しく復号できなくなってしまう, という問題がある.

そこで, 暗号化データに対して暗号化した状態で特定の演算処理を行うことで, 復号後に望んだ平文の処理結果を手に入れることができる, 準同型暗号が非常に注目されている.

Gentry や Dijk らにより暗号化したまま加法と乗法両方の演算が可能な完全準同型暗号が提案されて以降, 改良や応用に関する研究が活発に行われている.

本 PBL 演習では, 暗号化されたデータを安全に利活用するための準同型暗号に関する理論・応用・安全性について, 実際に実装することで習得する.

[学習目標]

準同型暗号の理論から応用・攻撃について学び, 実際に実装することで習得すると共に, 準同型暗号の有用性や実用化のための課題について体感する.

［講義計画］

(1) 数学からの準備と準同型暗号及びその応用に関する講義

知識単位：初等整数論，格子理論，準同型暗号，クラウドコンピューティング

(2) いくつかの準同型暗号の紹介

知識単位：RSA 暗号，Paillier 暗号，格子ベースの制限付き完全準同型暗号

(3) 準同型暗号の安全性に関する講義と攻撃

知識単位：(p−1)法，Learning With Errors (LWE)，格子攻撃

(4) 準同型暗号の応用と実装

知識単位：電子投票(匿名性の確保のみ)

(5) まとめと課題発表

［履修条件・受講条件］

「離散数学と計算の理論」か「実践情報セキュリティとアルゴリズム」の受講が望ましい．

また，数学的素養およびプログラミングの基本技術を必要とする．

［成績評価］

【評価の観点】準同型暗号やその応用と課題について実装や説明ができるか

学んだ準同型暗号の安全性について説明できるか

【評価方法】課題と最終プロジェクト

【評価基準】課題(60%) + 最終プロジェクト(40%)

［備考］

演習機材の関係で人数を制限します．

人数多数の場合には履修条件を満たしている学生から優先します．