6.5 実践安全な公開鍵暗号の設計と解読 PBL

[開講科目名]

(授業科目)高度セキュリティ PBL Ⅰ／(enPiT-Pro)実践安全な公開鍵暗号の設計と解読 PBL

[開講科目名(英)]

Advanced Security PBL I

[単位数] 1 単位

[開講日]

(調整中)

[担当教員]

宮地 充子(大阪大学), Chen-Mou Cheng(大阪大学)

[開講言語]

英語

[授業の目的・概要]

本科目では公開鍵暗号を用いてモノのインターネット(IoT)のデータを保護する方法を学び，実際に実装する方法について習得する.

サイバーセキュリティの基礎である暗号には共通鍵暗号および公開鍵暗号の二種類がある. 前者では各参加者は一つ以上の秘密鍵を事前に共有していることが仮定するので，n 端末のネットワークでは n^2 個の鍵を管理する必要があり,IoT への応用では現実的でない. 一方，公開鍵暗号は,n 端末のセキュアネットワークを 1 個の鍵で実現し，理論的に魅力的な解決方法を提供する. しかし，多くの IoT 機器は計算・メモリ・通信能力が非常に限られおり，公開鍵暗号を利用することが容易ではない. さらに，多数の IoT 機器を用いた攻撃も考えられる.

本 PBL 演習では IoT のデータを保護する公開鍵暗号の実現方法から暗号解読手法まで，理論的なアルゴリズム習得から，実際に実装する手法まで習得することを目的とする.

公開鍵暗号及びその解読手法を実装することで，暗号及び解読にかかる時間を実感することで，より深い理解を促すことを目的とする. 解読実験では並列化手法についても学習する.

[授業の目標]

現代の公開鍵暗号の背後にある理論，および資源に制約を持つ IoT 機器上で公開鍵暗号を実装する際に特有の課題について学ぶ. また，解読手法についても学ぶ. さらに IoT のための効率的な公開鍵暗号の実装方法とともに解読の実装方法や並列化手法についても学ぶ.

[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.

［講義計画］

(1) python の基本的な使い方

(2)暗号の基礎となる整数論及び必要なアルゴリズムの紹介と実装

知識単位：ユークリッドの互除法，バイナリ法

(3)公開鍵暗号の概念及 ElGamal 暗号の紹介と実装

知識単位：公開鍵暗号の概念, ElGamal 暗号， DH 鍵共有法

(4)典型的な解読方法 ρ法とその実装，並列化

知識単位：ρ法，指数計算法

(5)まとめと課題発表

［教科書・教材］

1. 宮地充子著,「代数学から学ぶ暗号理論」，日本評論社

［成績評価］

【評価の観点】IoT のための公開鍵暗号実装に必要な基礎知識

【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%)