2023年度MACS学生説明会

［SG2023-11］
暗号理論の数理と社会実装

参加教員：
伊丹 將人（SACRA 特定助教）
伊藤 哲史（数学･数理解析専攻 准教授）

動機

■高度情報社会の到来

・デジタル化
- 手紙 → メール･インスタントメッセンジャー
- 紙書籍 → 電子書籍
- 現金決済 → 電子決済

・デジタル化が進まないと思う理由１位：
「情報セキュリティやプライバシー漏えいへの不安があるから」

総務省(2021)「ウィズコロナにおけるデジタル活用の実態と利用者意識の変化に関する調査研究」

■暗号理論

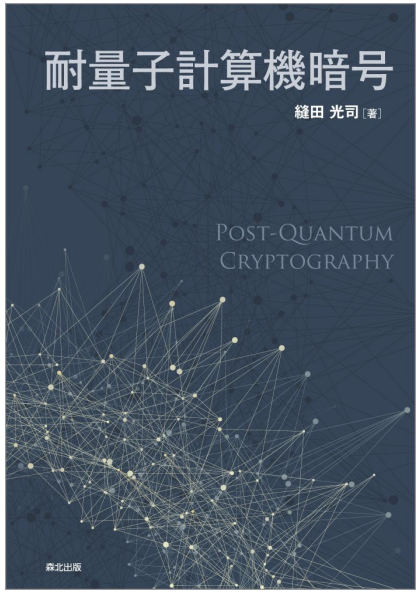
・公開鍵暗号
- 暗号化と復号に異なる鍵を用い、暗号化の鍵は公開する
- RSA暗号：大きな数の素因数分解が困難であることを利用

・Shorのアルゴリズムを使うと量子計算機で素早く素因数分解ができる
・量子計算機が完成したらどうやって安全性を担保するのか？

概要

■活動内容

・縫田光司[著]『耐量子計算機暗号』(森北出版)の輪講
  - 代数学×量子物理学×情報理論と分野横断的！
  - 暗号理論の中でも盛り上がっている！
・暗号理論を用いた技術・製品の紹介
  - Bitwarden, Signal, Proton, ...
・暗号理論の専門家を招いたセミナー
・暗号の実装



■実施期間

・前期(6月～7月)と後期(10月～1月)に隔週で90分程度
・曜日と時間帯は参加者で調整

■その他

・ハイブリッド形式で実施予定 (録画も参加者限定で公開予定)
・連絡や参加者同士の議論はElement (Messenger)を利用予定