2024年度MACS学生説明会

［SG2024-11］
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」

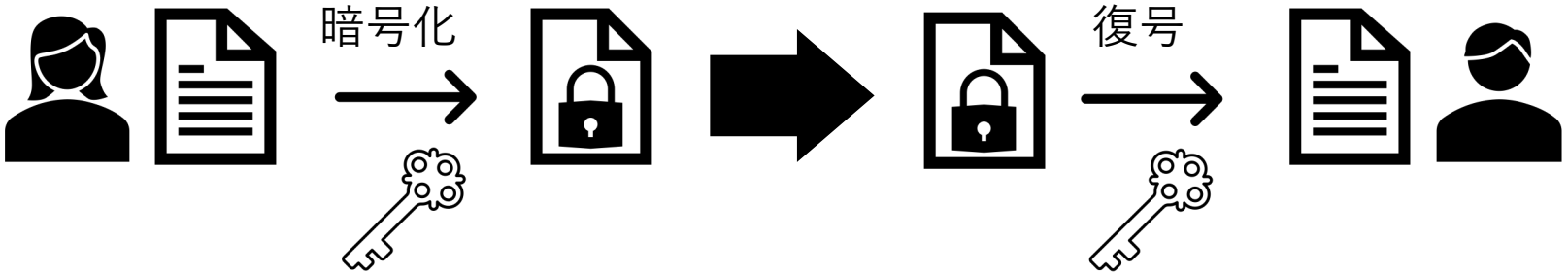
■漏洩事例

・LINEヤフー：LINE利用者の情報などが51万9千件漏洩した疑い(2023)
・京都大学：約4万人の個人情報が閲覧・取得可能(2021)

自分の身を守るには自分自身が適切な知識を身につけることも重要！

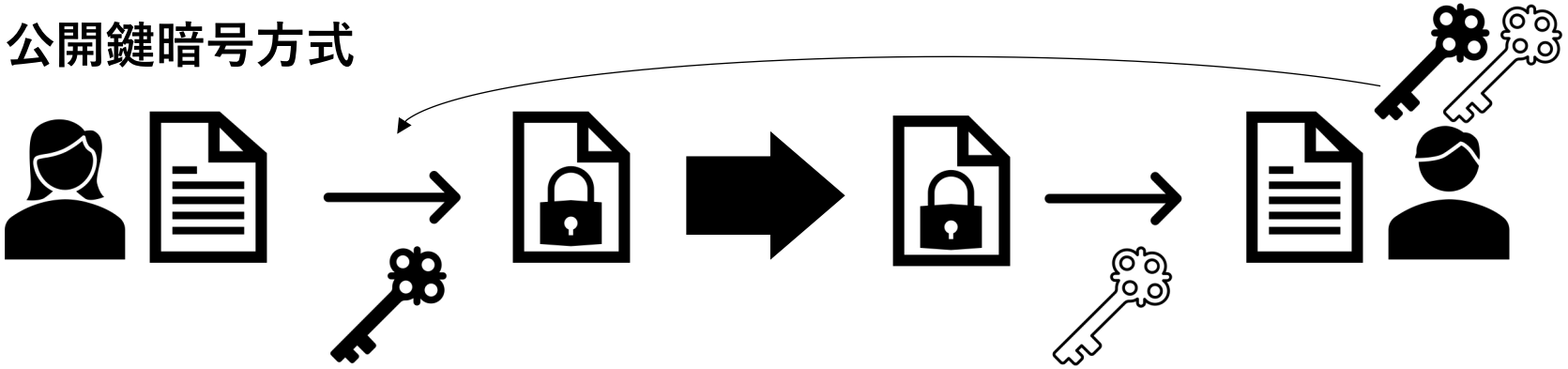
共通鍵と公開鍵

■共通鍵暗号方式



問題点：鍵の安全な共有が困難

■公開鍵暗号方式



問題点：公開する黒鍵から白鍵を予測不能にするのは難しそうだが....
→「解くのは難しいが答えの検証は容易な問題」があれば実現可能！

耐量子計算機暗号

■現在の公開鍵暗号における難しい問題

・大きな素数の積の素因数分解
・離散対数問題：整数a, gと素数pが与えられたとき$g^x \equiv a \bmod p$を満たすxを求める
・楕円曲線上の離散対数問題

問題点：量子コンピュータが使えると上記の**全て**の問題が効率的に解けてしまう

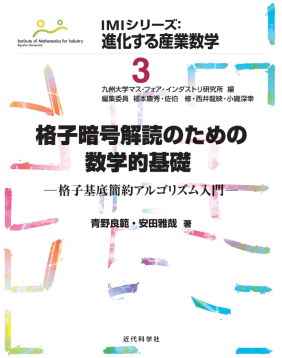
■耐量子計算機暗号

・**同種写像暗号**：楕円曲線間の写像の発見の困難性、鍵は小さいが処理が重い
→ 有望だったSIDHが古典アルゴリズムで破られた [https://eprint.iacr.org/2022/975]
・**多変数多項式暗号**：多変数2次多項式の求解困難性、鍵が大きい
→ 公開鍵暗号としては破られているものが多い、電子署名としては有望
・**符号ベース暗号**：ランダムな誤り訂正符号の復号困難性、鍵が大きい
→ 後述する格子暗号と比較して利点が少ない(?)
・**格子暗号**：高次元空間で最も近い格子点の発見困難性、現時点で最も有望
→ CRYSTALS-KyberがNISTの標準化計画で公開鍵暗号として唯一採択された
※ある種の格子暗号を破る量子アルゴリズムが発見(?) [https://eprint.iacr.org/2024/555]

活動の概要

■活動内容

・青野良範・安田雅哉[著]『格子暗号解読のための数学的基礎』（近代科学社）の輪講
・暗号理論を用いた技術・製品(Bitwarden, Signal,...)の紹介
・暗号理論の専門家を招いたセミナー
・（可能であれば）格子暗号の研究
・「2025年暗号と情報セキュリティシンポジウム」への参加



■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