暗号・情報セキュリティ研究室
西出研究室紹介
(当日研究室ブースでお待ちしています)

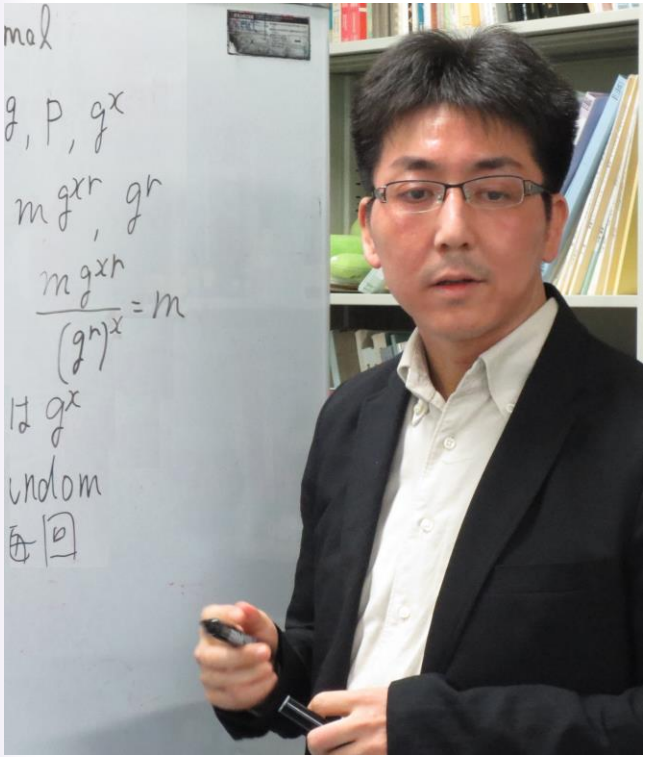
2022年

筑波大学
University of Tsukuba

メンバー構成

- スタッフ
  - 西出隆志 准教授
  - 面和成 准教授
  - 事務補佐員
- 学生(西出担当)
  - システム情報工学研究群 リスク・レジリエンス工学学位プログラム
    - 博士課程　3名
    - 修士課程　4名
  - 学部生
    - 2名（4年生）情報科学類
- 修了生の就職先の例
  - NEC研究所，富士通研究所, LINE, NTTドコモ, 野村総研，IIJ, セコム, GREE, 新日鉄住金ソリューションズ, etc

西出 隆志



- 准教授
- 専門：
  - 公開鍵暗号関連技術
  - 暗号プロトコル
  - プライバシ保護, etc

研究概要 [西出担当部分]

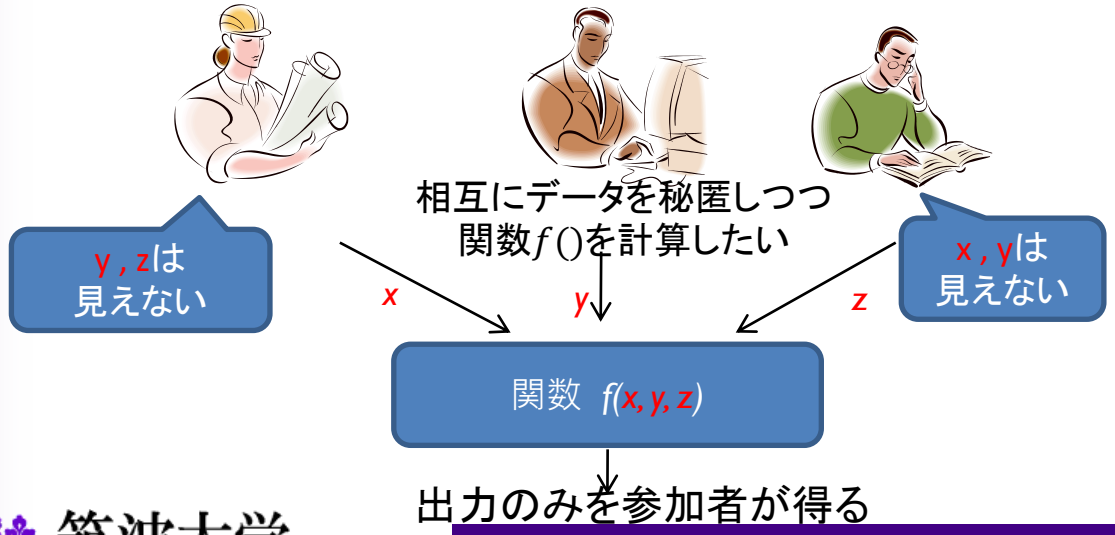
- 暗号の理論/基礎研究
  - 新しい(機能を持つ)暗号の提案やその効率化
  - 秘密データの単なる暗号化
    ⇒秘密データを扱う計算処理全体の暗号化へ
    - Data in Transit ➔ At Rest ➔ During Computation
- 暗号の応用研究 (プライバシ保護など)
  - 暗号を用いた新たな付加価値を持ったクラウドサービスやプロトコルの提案
  - 機械学習/ブロックチェーンへの利用
  - より具体的な利用シナリオを決めて効率化するなど

研究概要

- 公開鍵暗号，暗号プロトコル：
  - 公開鍵暗号代表例: RSA, ElGamal暗号
    - 研究では更に発展した暗号技術を扱う
      - 楕円曲線に基づく群構造を用いたPairing暗号
      - 耐量子格子(Lattice)暗号, etc
  - 従来の情報秘匿のみの機能を超え，情報を秘匿しつつ利用する機能を持つ高機能暗号技術
    - 秘密計算
    - 関数型暗号
    - 安全な計算委託
    - 完全準同型暗号
    - 量子計算機を利用する暗号
    - 暗号通貨の安全性/効率/利便性向上のための暗号基礎技術
    - Blockchain応用によるこれまで不可能だった暗号機能の実現
    - TEE (Trusted Execution Environment)の応用
      - Hardwareの仕組みに基づく安全性
      - Intel SGXなどのSecure CPU
  - 安全性モデルの定義とそれに基づく厳密な安全性証明

研究概要: 秘密計算

- 複数のデータを秘匿したままデータ処理
  ⇒プライバシ保護しつつデータ共有実現
  - 例: 個人情報を保護したままでのデータマイニング



- 効率的に実現するには?
- どんな安全性仮定が必要?
- 様々な秘密計算手法があるがどのように組み合わせればより効率的?
- 関数 $f()$ を具体的にしたら効率化可能?

…

筑波大学
University of Tsukuba

研究概要：関数型暗号，安全な計算委託

秘密データxからその暗号文 $[x]$ を作り，$[x]$への処理を委託 —$[x]$→ 自分のプログラム fとデータy使い $[x]$ を復号することなく $z \leftarrow f(x,y)$得る

秘密データxからプログラム $[f(x,\cdot)]$ を作り実行を委託 —$[f(x,\cdot)]$→ 自分の秘密データy を使い $z \leftarrow [f(x,\ y)]$ を実行して得る

- $[x]$や$[f(x,\ \cdot)]$から x が相手に漏れないようにできたら…
- $[f(x,\ \cdot)]$の実行回数を制限したいのだが…
- 2人でなく複数人が参加する状況にも適用したい…
- Ex. 機械学習のデータxをこのように外部委託したい…

⇒こういった課題を暗号技術で解決

研究概要: 完全準同型暗号，関数型暗号

- 完全準同型暗号 (Fully Homomorphic Encryption(FHE))
  - $E_{pk}(m_1) +_E E_{pk}(m_2) \rightarrow E_{pk}(m_1 + m_2)$
  - $E_{pk}(m_1) \times_E E_{pk}(m_2) \rightarrow E_{pk}(m_1 \times m_2)$
- 異なる鍵で暗号化されたデータを混ぜて処理なども可能(Multi-key FHE)
  - $E_{pk_1}(m_1) +_E E_{pk_2}(m_2) \rightarrow E_{pk_1,pk_2}(m_1 + m_2)$
  - $E_{pk_1}(m_1) \times_E E_{pk_2}(m_2) \rightarrow E_{pk_1,pk_2}(m_1 \times m_2)$
  - 復号にはpk_1, pk_2に対応する秘密鍵が必要
- 関数型暗号 (Functional Encryption)
  - $\mathrm{Dec}\left(sk_f,\ E_{pk}(m)\right) \rightarrow f(m)$
- データ復号無しに様々な処理が可能
  - 困難であった秘密データの共有利用などを可能に
  - 実用化には更なる効率化が必要

研究概要: これまでの研究テーマ例

- 既に配布した鍵を持っている人たちの一部のみを後から失効し，失効された人は新たに生成された暗号文が復号できなくなる属性ベース暗号方式
- 暗号データに対してあいまいな検索条件(例: 080-????-1111)の指定が可能な検索可能暗号方式
- 実行回数が暗号と分散クラウドストレージにより安全に制限されたプログラムとその電子現金方式への応用
- 完全準同型暗号の効率化
- 完全準同型暗号を用いた暗号データ同士の大小比較, 除算
- Blockchainを利用し，公開鍵に対する秘密鍵が漏洩したとしても，過去の盗聴された暗号文を復号させない公開鍵暗号方式

最後に

- 暗号と情報セキュリティは、縁の下の力持ちで見えないことが多いですが社会の基盤技術として広まっています
- 情報技術が世の中に広まり、定着するにつれ、暗号と情報セキュリティは欠かせない要素技術として存在し続けることでしょう
- 数学的に厳密な安全性解析に基づく強い&高機能な暗号技術で世の中の安全に貢献しましょう