I486S 暗号プロトコル理論
- 秘密計算-

導入 4/17

講師　藤﨑英一郎

I486S のことあれこれ

- 開講スケジュール
  - 毎週火曜日 5 限 (17:10—18:50) 1-1, 2-1 横断
  - 予定の14回: 4/17, 4/24, 5/1, 5/15, 5/22, 5/29, 6/5, 6/19, 6/26, 7/3, 7/10, 7/17, 7/24, 7/31.
- JAIST学生用情報
  - 履修登録：教務係からきたメールに4/25 (17:00)までに返信（学務システムからは申請できません）
  - H29年度情報セキュリティプログラム申請者：
    - I471S情報セキュリティ演習（廃止） --> I486S暗号プロトコル理論（代用）
    - 情報セキュリテイプログラム修了 = SecCap6修了

I486Sの講義内容

- 近年、国内外の大学、企業の研究所で実装実験が盛んに行われている秘密計算の理論について講義をする
- 秘密計算とは、複数の参加者が各自持つ秘密を漏 らさず、しかしその秘密から計算できる計算結果のみを協力して計算する暗号プロトコル
- 本講義では、計算量的仮定を一切必 要としない情報理論的に安全なマルチパーティ計算の基本テクニック（BGW[3]系）と、二者間の計算量的仮定を必要とする Yao の秘密計算プロトコル（Yao[6]）を中心に解説する

H30年度情報セキュリティプログラム専門科目 (I4xxS) の紹介

- I486S「暗号プロトコル理論」(毎週火曜日、4/17開始、1-1,1-2期)
  - 近年、国内外の大学、企業の研究所で実装実験が盛んに行われている秘密計算の理論について講義をする
  - 秘密計算とは、複数の参加者が各自持つ秘密を漏 らさず、しかしその秘密から計算できる計算結果のみを協力して計算する暗号プロトコル
  - 本講義では、計算量的仮定を一切必 要としない情報理論的に安全なマルチパーティ計算の基本テクニックと、二者間の計算量的仮定を必要とする Yao の秘密計算プロトコルを解説する
- I465S「情報セキュリティ運用リテラシー」 (IISEC配信、10/3~)
  - 暗号、システム技術、ネットワーク技術から法制度にわたる、幅広い基礎知識を学ぶとともに、基礎知識学習などを通 して体験的に学習したセキュリティ技術が実社会においてどのように役立っているかについて、技術から実用化の縦方向での知見 を深める
- I466S「最新情報セキュリティ理論と応用」 (阪大配信、10月～)
  - RFID タグや携帯端末等，IoT 機器におけるデータ秘匿やデータの偽造を防ぐ技術として脚光を浴びている楕円曲線暗号について解説するとともに、その 実装も行う。応用編では、セキュリティが利用・導入されているシステム、製品の課題等を学ぶ
  - 現代のアルゴリズムにおいて必要不可欠となった計算に乱数を活用する乱択アルゴリズムについて学習する。特にその基本的な設計技術および確率的な 解析手法を学ぶ

秘密計算に関するプレスリリースや記事

- NTT、秘密分散技術が国際標準化機構の国際標準において標準技術として採択
- NEC、産総研が秘密計算を実用化 データの中身を秘匿し、統計分析
- 秘密分散・秘密計算システム - 一橋大学社会科学統計情報センター
- NEC、機密情報の漏えいを強固に防止する秘密計算の高速化手法を開発
- 暗号化したままデータ分析を行う秘匿分析技術を開発 - 日立製作所
- NEC、機密情報の漏えいを強固に防止する秘密計算の高速化手法を開発
- NEC・富士通・日立に見る「マテリアルズ・インフォマティクス」最前線
- 複数の研究機関が持つゲノムデータを相互に開示せず分析する解析手法を開発

授業の進め方、勉強の仕方

- 教科書は無し（ただし後述する参考文献にかなり忠実に沿う）
- 授業：スライドと板書
- 勉強法：講義を聞き、講義後 にアップされた授業の資料 (https://www.jaist.ac.jp/~fujisaki/ からリンク) を復習
- 出欠：出欠はとる
- 評価方法：レポート*

*：秘密計算についてのリテラシーが身についたかが合否の基準

参考文献

- [1] Ronald Cramer, Ivan Bjerre Damgård, and Jesper Buus Nielsen: Secure Multiparty Computation and Secret Sharing, Cambridge University Press (ISBN 9781107043053).
- [2] R. Cramer, I. Damgaard, J. Nielsen: Multiparty computation, Introduction, https://pdfs.semanticscholar.org/6ae2/38ab990dd0c97fa972dc6087da7aaece4279.pdf
- [3] M. Ben-Or, S. Goldwasser and A. Wigderson: Completeness Theorems for Non-Cyptographic Fault-Tolerant Distributed Computation, in STOC88, pp. 1--10.
- [4] Ronald Cramer, Ivan Damgaard and Ueli M. Maurer: General Secure Multi-party Computation from any Linear Secret-Sharing Scheme, in EUROCRYPT2000, pp 316--334.
- [5] Ronald Cramer, Ivan Damgaard and Yuval Ishai: Share Conversion, Pseudorandom Secret-Sharing and Applications to Secure Computation, in TCC2005, pp 342--362.
- [6] A. Yao: Protocols for secure computations, in FOCS82, pp 160--164.
- [7] Yehuda Lindell and Benny Pinkas: A Proof of Security of Yao's Protocol for Two-Party Computation, Journal of Cryptology, volume 22(2), pp.161--188, 2009.

秘密計算

x_3

x_2

x_4

x_1

x_5

各人の秘密：　$x_1, \ldots, x_5$

事前に共有：　関数　f

プロトコルの最後に各参加者が得たいもの*：

計算結果　$f(x_1, .., x_5)$

Privacy：

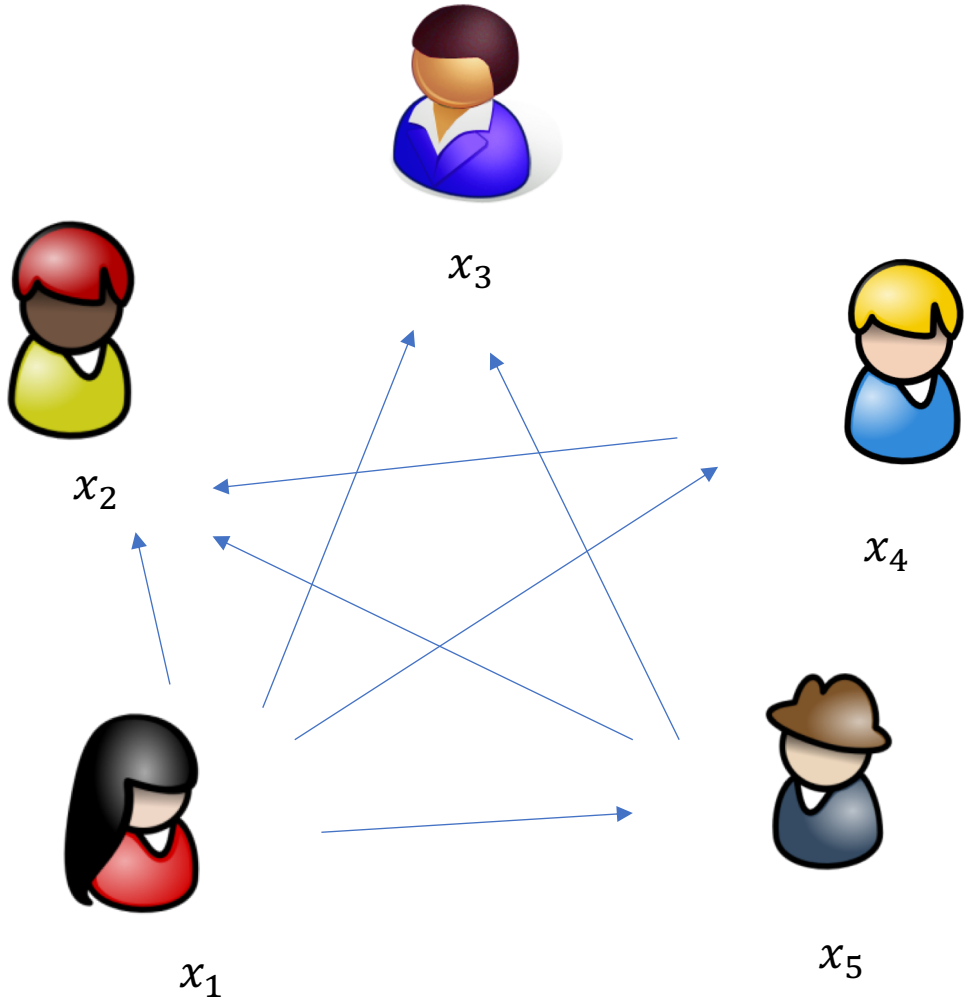
計算結果から漏れるもの以外は漏らさない**

Robustness：

不正者が計算結果を違うものに変えられない***

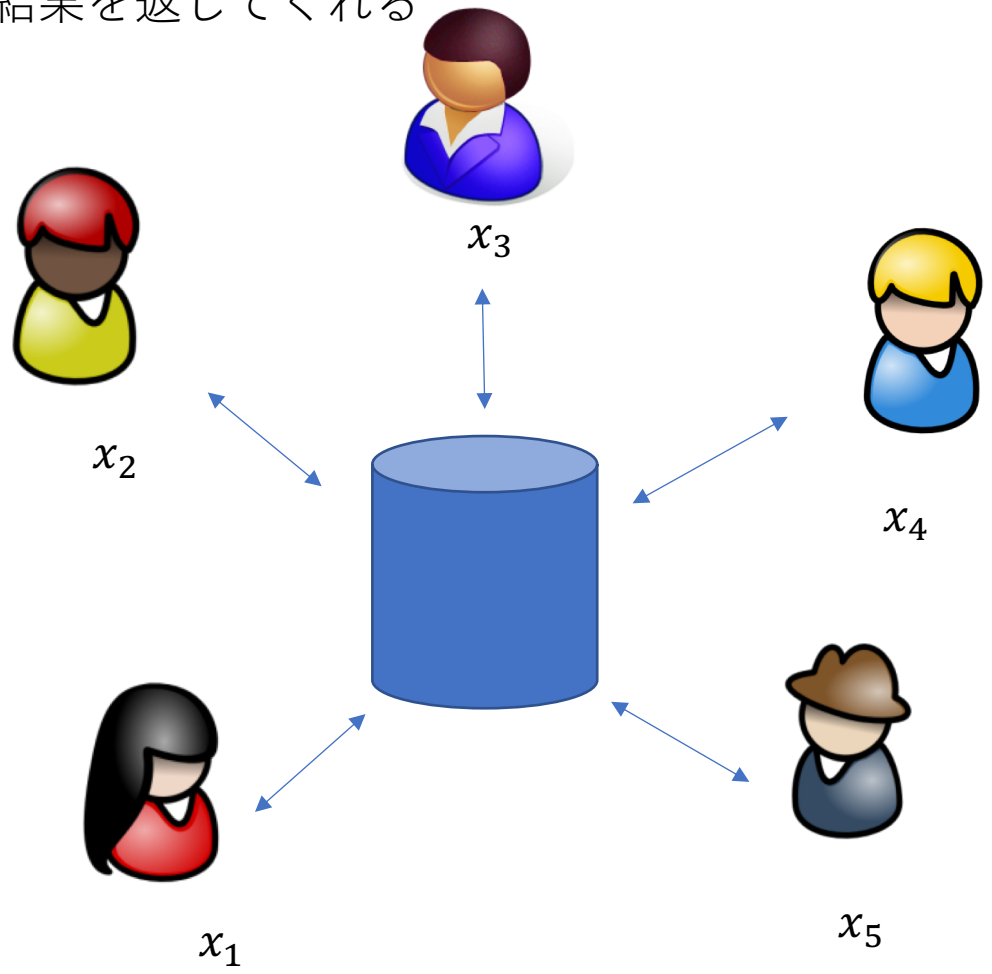
秘密計算

現実のプロトコル



理想状態

箱があって、各自の秘密x_iを預けると
計算結果を返してくれる



ネットワークモデル

- どのプレーヤ同士もpeer-to-peer で秘密通信可
  - 秘密通信 (secure channel)
- Synchronous （同期）
  - 送られた情報は遅延なく、次のスロットで相手に必ず届く
  - Opp. Asynchronous（非同期）
- 同報通信を仮定する場合もある
  - 同報通信を仮定しない場合、同報通信はByzantine 合意を用いて実現する

不正者に関する決め事

- 不正者の呼称
  - 敵 (adversary) ともいう
- （多くの場合は）不正者の数を制限（この講義でも）
  - 参加者n人の中、不正者は高々t人まで
  - 不正者は全員結託していると考える
- 不正者のタイプ：大きく分けて二通り
  - Passive 不正者
    - Honest-but-curious, semi-honest などとも言う
    - プロトコルを逸脱はしないが、自分の得た情報から他のプレーヤの情報を盗もうとする
  - Active 不正者
    - プロトコルを好きなように逸脱して、他のプレーヤの情報を盗む。プロトコルを邪魔して正直なプレーヤ達が計算結果を得ることを妨げる
    - さらに、static/adaptive に分類される

不正者数に対して知られている結果

	Passive	Active w/ Broadcast	Active w/o Broadcast
情報理論的安全性	$< n/2$	$< n/3$	$< n/3$
統計的安全性	$< n/2$	$< n/2$	$< n/3$
計算量的安全性	n	$<n/2$	$<n/2$

n=2の時は、とりあえず除外

本講義で主に扱う秘密計算方式（BGW/CCD型）

- 情報理論的安全な三者以上の秘密計算プロトコル（＝マルチパーティプロトコル (MPC)）
- 文献 [2] に解説：BGW[3]/CCDを基にしたCDM[4]方式
  - Passive 安全性：不正者数 < n/2
  - Active 安全性：不正者数< n/3
- 主要テクニック
  - 線形 (linear) 秘密分散 (secret sharing): LSS
    - 実際は、Shamir’s Secret Sharing.
  - 検証可能 (verifiable) 線形秘密分散 (VSS): VLSS
    - BGW 型
  - (V)LSSでの掛け算
    - 足し算は容易なので（それが線形の意味）掛け算をするテクニックが重要
    - 足し算、掛け算が出来るとブール代数を計算でき論理回路を作れる

本講義で主に扱う秘密計算方式（Yao）

- 計算量的に安全な２者に特化した秘密計算プロトコル (=2PC)
- Yao[6]方式
- 主要テクニック
  - Garbled Circuit（ガーブルドサーキット）
  - Oblivious Transfer（曖昧通信路）
  - Zero-Knowledge Interactive Proofs（ゼロ知識証明）
    - Passive 安全性を言うならゼロ知識証明は不要

本講義で扱わない秘密計算

- 完全準同型暗号を用いたタイプ

その他

- Byzantine 合意とか
- 論理回路とか
- 有限体とか
- 体上の演算からブール計算とか

$b, b' \in \{0,1\}$

$b \wedge b' \iff b \cdot b'$

$b \vee b' \iff b + b' - b \cdot b'$

$\neg b \iff 1 - \mathrm{b}$

講義計画

1. 秘密計算(導入)
2. 秘密分散(1)
3. 秘密分散(2)
4. マルチパーティ計算(耐受動的攻撃者安全性)(1)
5. マルチパーティ計算(耐受動的攻撃者安全性)(2)
6. 検証可能秘密分散(1)
7. 検証可能秘密分散(2)
8. マルチパーティ計算(耐能動的攻撃者安全性)(1)
9. マルチパーティ計算(耐能動的攻撃者安全性)(2)
10. マルチパーティ計算(耐能動的攻撃者安全性)(3)
11. (複製秘密分散ベースによる)別手法の構成
12. 二者間秘密計算の基本技術(ガーブルドサーキットと曖昧通信)
13. 二者間秘密計算(耐受動的攻撃者安全性)
14. まとめ