新技術説明会
New Technology Presentation Meetings!

安全で高速な秘匿計算のための秘匿演算変換

広島市立大学
大学院情報科学研究科　情報工学専攻
准教授　上土井　陽子

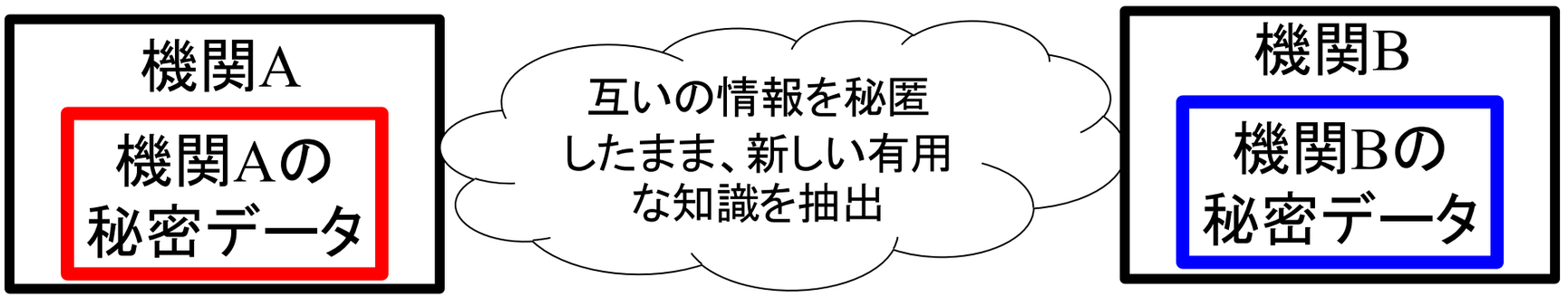
3つのひかり　未来をつくる
広島市立大学
Hiroshima City University

2025年12月9日

研究背景

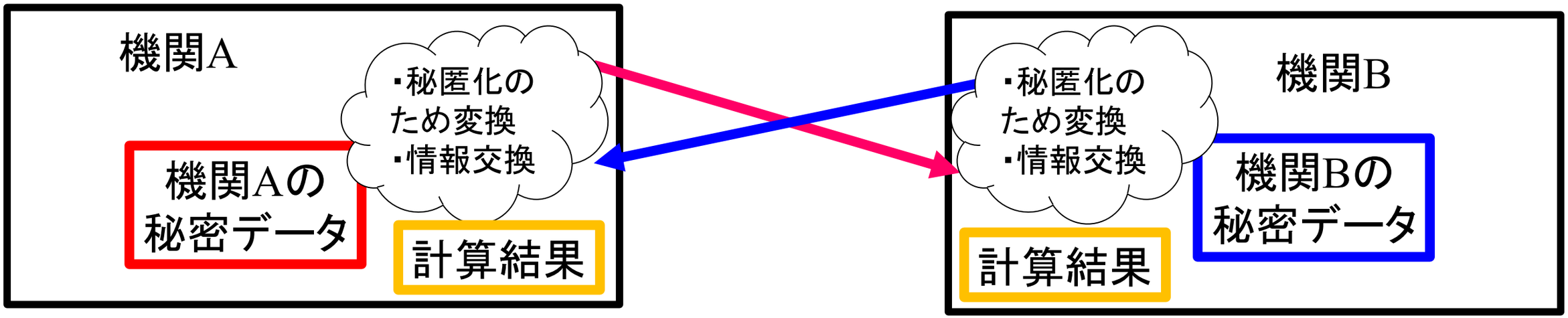
- 企業などに集積された膨大な個人データの利活用が注目
- 個人データはプライバシー保護の観点から秘密データ
- 競合する複数の機関が一時的、もしくは、部分的に協力することで互いの秘密データから新しい知識を導出可能

注目技術：プライバシー保護データマイニング



秘密計算

- プライバシー保護技術の一つ
- 複数の機関がそれぞれ保持している秘密データを入力として計算を行なった時の結果を互いの情報を明かすことなく、求めること
- 利用技術：暗号技術(準同型暗号), 秘密分散法



従来技術とその問題点（1）

- 代表的な従来技術１[準同型公開鍵暗号]
  - ✓暗号文に対して演算を適用することで、平文に演算を施せる準同型暗号が存在
  - ✓完全準同型暗号(加法・乗法)：Paillier暗号、ElGamal暗号
  - ✓公開鍵暗号で非対称な暗号方式のため、計算コスト大
  - ✓連続的な計算や大きな値の計算には注意を要する
  - ✓各演算操作を暗号文に対する高価な演算(例：加算→乗算、乗算→べき乗算)で実行する必要がある
  - ✓量子コンピュータにより暗号が解読される可能性

従来技術とその問題点（2）

- 代表的な従来技術２[秘密分散法]
  - ✓秘密を複数のシェアと呼ばれる情報に分散し、後にシェアを集めて秘密を再構築する方法
  - ✓複数のシェアに分散する場合には３者以上間でないと機密性を確保できない
  - ✓加算が主な演算であり乗算には注意を要する

新技術の特徴･従来技術との比較

- ２者間で秘密計算を高速に、かつ、安全に実施するための新しい秘匿演算変換という枠組みを開発
- 演算変換とは２つの入力X,Yをそれらに演算Aを実行したときの解をZとすると、演算Bを実行してZを得られるような２つの値Φ,Ψ に変換すること
- 複数の演算を利用する秘密計算の一部の演算を他の演算に変換し、秘密計算を安価なコストをもつ計算に変換
- 安全性の根拠が従来の準同型公開鍵暗号とは異なり、意味のある情報(交渉秘密情報)の安全性による

新技術説明会
New Technology Presentation Meetings!

提案技術の一例

前提条件

機関P1の秘密情報

$X,\ Secret\_In\_X,\ Secret\_Out\_X$

共通情報

関係　$Secret\_In\_X \cdot Secret\_In\_Y = Secret\_Out\_X + Secret\_Out\_Y$

機関P2の秘密情報

$Y,\ Secret\_In\_Y,\ Secret\_Out\_Y$

秘匿演算変換処理

機関P1

送信情報　$CA = X + Secret\_In\_X$

機関P2の情報受信後内部計算

$$\begin{aligned}\Phi &= CB \cdot X + Secret\_Out\_X \\ &= (Y + Secret\_In\_Y) \times X + Secret\_Out\_X \\ &= X \cdot Y + X \cdot Secret\_In\_Y + Secret\_Out\_X\end{aligned}$$

機関P2

送信情報　$CB = Y + Secret\_In\_Y$

機関P1の情報受信後内部計算

$$\begin{aligned}\Psi &= -CA \times Secret\_In\_Y + Secret\_Out\_Y \\ &= -(X + Secret\_In\_X) \times Secret\_In\_Y + Secret\_Out\_Y \\ &= -X \cdot Secret\_In\_Y - Secret\_In\_X \cdot Secret\_In\_Y + Secret\_Out\_Y\end{aligned}$$

プロトコル適用後成立する関係：X･Y＝ Φ＋ψ

$$\begin{aligned}\Phi + \Psi &= X \cdot Y + X \cdot Secret\_In\_Y + Secret\_Out\_X - X \cdot Secret\_In\_Y + Secret\_Out\_Y - Secret\_In\_X \cdot Secret\_In\_Y \\ &= X \cdot Y\end{aligned}$$

新技術説明会
New Technology Presentation Meetings!

提案技術の適用例（ベクトル内積計算）

前提条件

機関P1の秘密情報

秘密入力ベクトル $(X_1, X_2, \dots, X_n)$

$Secret\_In\_X_i, Secret\_Out\_X_i \ (1 \le i \le n)$

共通情報

関係 $Secret\_In\_X_i \cdot Secret\_In\_Y_i = Secret\_Out\_X_i + Secret\_Out\_Y_i \ (1 \le i \le n)$

機関P2の秘密情報

秘密入力ベクトル $(Y_1, Y_2, \dots, Y_n)$

$Secret\_In\_Y_i, Secret\_Out\_Y_i \ (1 \le i \le n)$

秘匿演算変換処理

機関P1

送信情報

$CA_i = X_i + Secret\_In\_X_i \ (1 \le i \le n)$

機関P2の情報受信後内部計算

$\Phi_i = CB_i X_i + Secret\_Out\_X_i \ (1 \le i \le n)$

機関P2

送信情報

$CB_i = Y_i + Secret\_In\_Y_i \ (1 \le i \le n)$

機関P1の情報受信後内部計算

$\Psi_i = -CA_i Y_i \cdot Secret\_In\_Y_i + Secret\_Out\_Y_i \ (1 \le i \le n)$

プロトコル適用後成立する関係

$$(X_1, X_2, \dots, X_n) \cdot (Y_1, Y_2, \dots, Y_n) = \sum_{1 \le i \le n} \Phi_i + \sum_{1 \le i \le n} \Psi_i$$

想定される用途

- 暗号化ニューラルネットワークによる秘密データ解析
  - 人工知能の技術である深層学習や行列分解などが大規模なデータに対して利用されている
  - データやパラメータをベクトルで管理し、それらのベクトル間の内積の値によりデータを分類する
  - データが秘匿すべき個人情報であったり、パラメータ値が機関にとって重要な秘密情報である場合には両方の情報を暗号化した上で秘密計算にて判定
  - 本発明技術を利用することで、高速で、かつ、安全な計算が可能

実用化に向けた課題

- 現在、交渉秘密情報を作成する方法を複数検討中
- 暗号化ニューラルネットワークでの実験的性能評価
- 内積計算以外の秘密計算での適用

企業への期待と貢献

- 複数の企業間で安全な情報共有を実施したい企業との共同研究を希望
- 安全な交渉秘密情報を提供するサービスのビジネスモデルの検討
- 開発技術を利用したプライバシー保護データマイニング基盤の構築

本技術に関する知的財産権

- 発明の名称　：秘匿演算変換システム、秘匿演算変換方法、および、秘匿演算変換プログラム
- 出願番号　　：特願2018-139191
- 出願人　　：公立大学法人広島市立大学
- 発明者　　：上土井陽子、若林真一

お問い合わせ先

広島市立大学
地域共創センター
産学連携コーディネータ

ＴＥＬ：082-830-1545
e-mail: ken-san@m.hiroshima-cu.ac.jp