Privacy-Preserving Cooperative Computations

Wenliang (Kevin) Du
Mikhail J. Atallah
CERIAS
Purdue University

duw@cerias.purdue.edu

Secure Multi-Party Computations (SMC)

Alice

Bob

\( x \) \rightarrow\n
\( y \) \rightarrow\n
Computation

\( \rightarrow \) \rightarrow\n
\text{result} \rightarrow

\{ \text{comparison, bidding, voting, signing, ...} \}
Theoretical Results and Motivation

- General SMC problem is solvable
  - Yao('86), Goldreich('87), Kilian('88)
  - Circuit evaluation
- Theoretical result is not efficient
  - Goldreich
  - e.g. a multiplication circuit is quadratic in the size of its inputs.
- Specific SMC problems need special solutions

Privacy-Preserving Statistical Analysis

- Traditional Statistical Analysis:
  - Data set: \{(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)\}
  - Compute mean, standard deviation, correlation coefficient, regression, etc.
- New Problem 1
  - Alice has \((x_1, y_1), \ldots, (x_k, y_k)\)
  - Bob has \((x_{k+1}, y_{k+1}), \ldots, (x_n, y_n)\)
- New Problem 2
  - Alice has \((x_1, x_2, \ldots, x_n)\)
  - Bob has \((y_1, y_2, \ldots, y_n)\)
Privacy-Preserving Scientific Computations

- Solve $Mx = b$
- Solve
  $$\begin{pmatrix} M_1 \\ M_2 \end{pmatrix} x = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$$
- Solve $[ M_1 \ M_2 ] x = b$
- Solve $( M_1 + M_2 ) x = b_1 + b_2$

Privacy-Preserving Scientific Computations (cont’d)

- Linear System of Equations
  - $Mx = b$, $M$ is $n$ by $n$ matrix
- Linear Least-Square Problems
  - $Mx = b$, but $M$ is $m$ by $n$ matrix, $m > n$
- Linear Programming Problems
  - minimize $f(x) = c^T x$: $Mx \leq b$, $0 \leq x$
Privacy-Preserving Geometric Computations

- Point Inclusion Problem
- Intersection Problem

Privacy-Preserving Data Mining

- Data Mining:
  - Classification
  - Data clustering
  - Association rules
  - Data generalization
  - etc.
Privacy-Preserving Data Mining

Database

Privacy-Preserving Database Query

Alice

Bob

Query

Result

Private Database Model

Public Database Model
Summary of Our Results

- Privacy-Preserving Scientific Computations
- Privacy-Preserving Statistical Analysis
- Privacy-Preserving Geometrical Computations
- Privacy-Preserving Database Query

Future Work

- Other Interesting SMC Problems
  - Cooperative Machine Learning
  - Cooperative Intrusion Detection
  - Information Retrieval
- SMC problems in E-commerce
  - Business to Business operations
  - Business to Customer operations