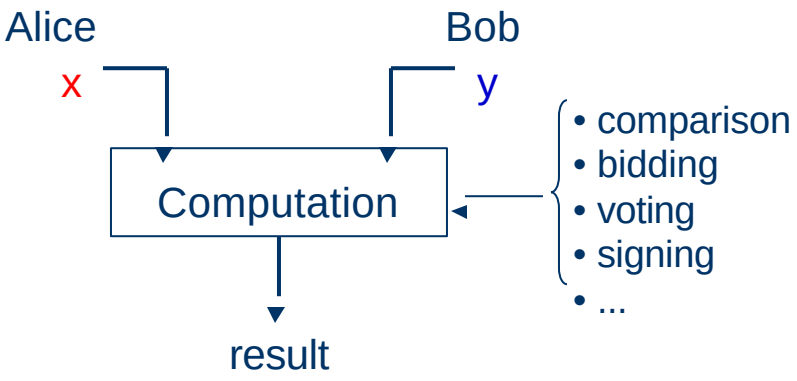
Privacy-Preserving Cooperative Computations

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

duw@cerias.purdue.edu

1

Secure Multi-Party Computations (SMC)



2

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

3

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 $(y_1, y_2, \ldots, y_n)$

4

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 $(M_1 + M_2)\, x = b_1 + b_2$

5

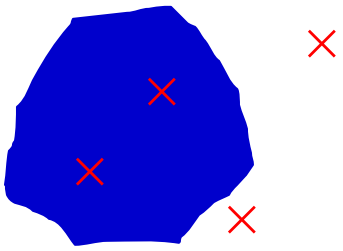
Privacy-Preserving Scientific Computations (cont'd)

- 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 $\mathbf{f(x)=c^T x}$: $\mathbf{Mx} \leq \mathbf{b}$, $\mathbf{0} \leq \mathbf{x}$

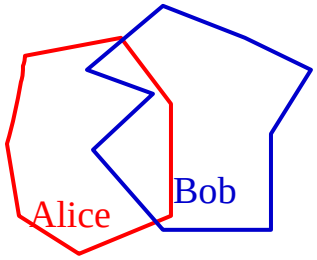
6

Privacy-Preserving Geometric Computations

- **Point Inclusion Problem**

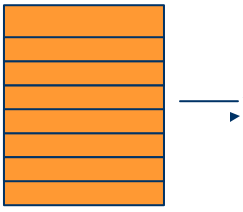


- **Intersection Problem**



7

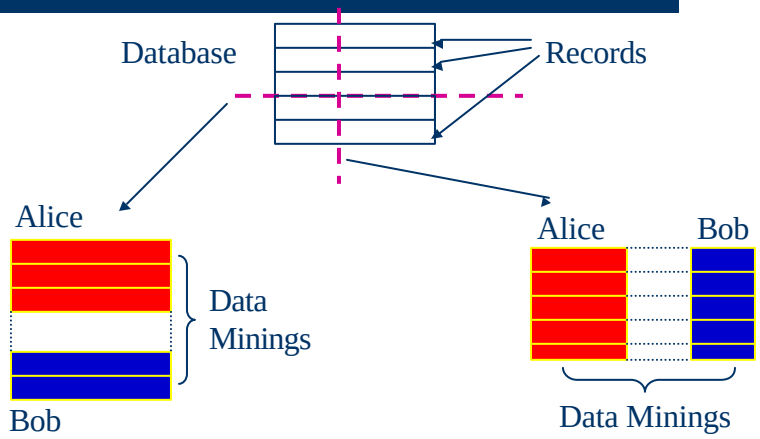
Privacy-Preserving Data Mining



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

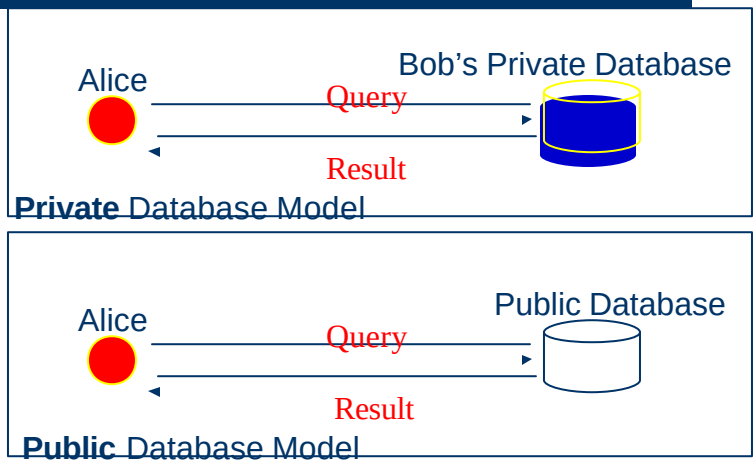
8

Privacy-Preserving Data Mining



9

Privacy-Preserving Database Query



10

Summary of Our Results

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

11

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

12