Models for Privacy-Preserving Collaboration

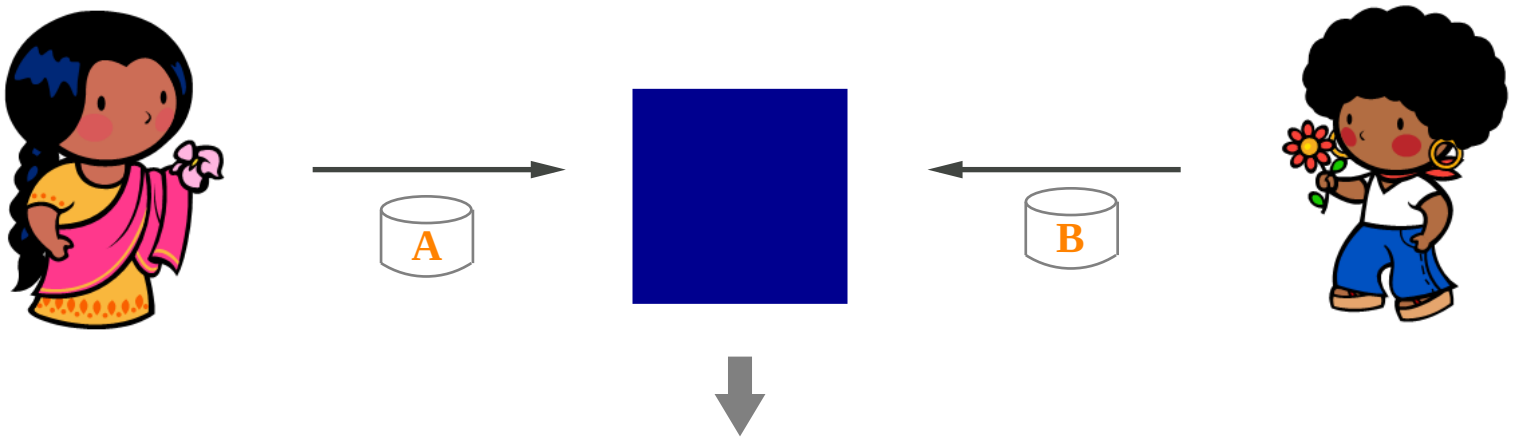
Wei Jiang

Department of Computer Science
Purdue University, West Lafayette, Indiana

14th April 2007

PURDUE UNIVERSITY

Data Confidentiality and Personal Privacy in Distributed Environment



PURDUE UNIVERSITY

Secure Distributed k-Anonymity

Age	Gender
23	M
35	M
24	F
27	F
40	M
26	M

Zip code	Occupation
48502	Research Assistant
60616	Assistant Professor
47906	Teaching Assistant
47405	Teaching Assistant
60607	Associate Professor
48502	Research Assistant

Age	Gender	Zip code	Occupation
[20, 30]	M	48502	Research Assistant
[35, 40]	M	606**	Professor
[20, 30]	F	47***	Teaching Assistant
[20, 30]	F	47***	Teaching Assistant
[35, 40]	M	606**	Professor
[20, 30]	M	48502	Research Assistant

PURDUE UNIVERSITY

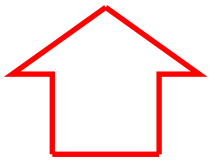
Basic Definitions of Secure Function Evaluation

Adversary Models

- Semi-honest: follow the rules of the protocol using correct input, but is free to compute anything based on what has been seen
- Malicious: behave arbitrarily to compromise privacy

PURDUE UNIVERSITY

Accountable Computing Framework - Check after the Fact



PURDUE UNIVERSITY

Non-Cooperative Computing

Example (Computing Sample Mean of x, y)

- Alice: x; Bob: y and y', where y' Bob's modified input
- Given y, y' and incorrect sample mean μ' (based on x, y'), Bob can obtain the correct μ

$$\mu' = \frac{x + y'}{2} \quad \Rightarrow \quad \mu = \mu' + \frac{y - y'}{2}$$

PURDUE UNIVERSITY

Non-Cooperative Computing

Example (Computing Sample Mean of x, y)

- Alice: x; Bob: y and y', where y' Bob's modified input
- Given y, y' and incorrect sample mean μ' (based on x, y'), Bob can obtain the correct μ

$$\mu' = \frac{x + y'}{2} \quad \Rightarrow \quad \mu = \mu' + \frac{y - y'}{2}$$

PURDUE UNIVERSITY

Future Work

Secure Distributed k-Anonymity

- More efficient protocols
- Multi-party (more than two) protocol

Accountable Computing Framework

- Formalize the AC-framework
- Remove the third party verifier
- Extend the framework for more than two parties

Non-Cooperative Computing

- Composition theorem
- Design of SFE-NCC protocols

PURDUE UNIVERSITY