Secure Multiparty Computation

Brett Hemenway
University of Pennsylvania

April 22nd, 2015
Secure Multiparty Computation (MPC)

A MPC protocol is represented by the function $f(x, y)$. Nothing about $x$ and $y$ is revealed beyond $f(x, y)$. The diagram shows two parties, one thinking of $x$ and the other thinking of $y$. They compute $f(x, y)$ without revealing $x$ or $y$.
Secure Multiparty Computation (MPC)

Nothing about $x$ and $y$ is revealed beyond $f(x, y)$. 

MPC protocol
Secure Multiparty Computation (MPC)

Nothing about $x$, $y$ is revealed beyond $f(x, y)$.
Secure Multiparty Computation (MPC)

Nothing about $x, y$ is revealed beyond $f(x, y)$
Properties of MPC

- MPC is a cryptographic alternative to a trusted party
- In principle, MPC can compute any function
- MPC provably hides everything except the outcome (MPC does not protect against inferential disclosure)
- Algorithms are public, can be open-source (well-studied by the cryptographic community)
Proposed Applications of MPC

- Financial oversight
  - [AKL12, FKOS13, BTW12]
  - MPC can compute global properties of the financial network while hiding individual portfolios and investment strategies

- Secure statistics
  - [DA01b, DA01a, DA01c, DCH04, DHC04, LP09, BNTW12, BKLS14, BKL^14]
  - Data owners can compute statistics across joint data sets without sharing their data sets with each other (or any outside party)
Proposed Applications of MPC

- Biology and medicine
  - [Zel14, CH15, KBLV13]
  - Genome-wide association studies
  - Analyze long-term trends when insurers may have only short-term data on patients
  - Analyze global patterns when hospitals have only local data

- Conjunction analyses
  - [HWB14, KW14]
  - Satellite owners can calculate the probability their satellites will collide without revealing their positions

- Hazard analyses
  - [GHWB14]
  - Create virtual database of “anomalies” without sharing failure information
  - Create virtual database of cyber-attacks / data breaches without sharing penetration information
  - Create virtual hazard database without sharing damage and response information
3-Server BGW Implementation
The Sharemind System from Cybernetica

http://sharemind.cyber.ee/
Statistics across multiple databases

[BKLS14, BKL$^+$14]

- **Data:**
  - Linking Tax and Education data
    - Tax and Customs Board
    - Ministry of Education and Science

- **Statistics:**
  - $t$-tests
  - Wilcoxon Rank Sum Test
  - $\chi^2$ tests
Moving Forward

Cryptographers are looking for use-cases

Where can we use MPC to facilitate analysis and collaboration?


References II

Dan Bogdanov, Margus Niitsoo, Tomas Toft, and Jan Willemsen.
High-performance secure multi-party computation for data mining applications.

Dan Bogdanov, Riivo Talviste, and Jan Willemsen.
Deploying Secure Multi-Party Computation for Financial Data Analysis.

Erika Check Hayden.
Extreme cryptography paves way to personalized medicine.


David A. Galvan, Brett Hemenway, William Welser, and Dave Baiocchi.

Brett Hemenway, William Welser, and Dave Baiocchi.
Achieving Higher-Fidelity Conjunction Analyses Using Cryptography to Improve Information Sharing.

Liina Kamm, Dan Bogdanov, Sven Laur, and Jaak Vilo.
A new way to protect privacy in large-scale genome-wide association studies.
Liina Kamm and Jan Willemsen.  
Secure floating point arithmetic and private satellite collision analysis.  

Yehuda Lindell and Benny Pinkas.  
Secure Multiparty Computation for Privacy-Preserving Data Mining.  

Nicholette Zeliadt.  
Cryptographic methods enable analyses without privacy breaches.  