CERIAS

Secure Computational Outsourcing

Jiangtao Li Mikhail Atallah

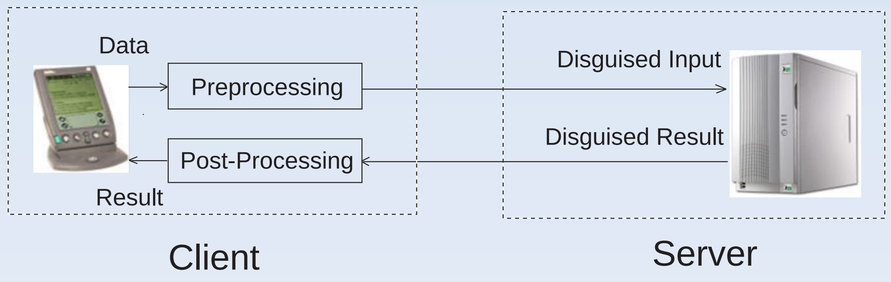
Motivation

- Need for outsourcing
  - A computer gets large computing resource from Grid or Supercomputers
  - A weak PDA, Smartcard, or sensor needs help from untrusted workstations
- Need for preserving privacy
  - Input data is sensitive
  - Result is also sensitive
- Secure Outsourcing
  - Client outsources the computation to Server
  - Server learns nothing about real input and output

Related Work

- Server Aided Secret Computation
  - A smartcard computes modular exponentiation with the help of a server
  - Server cannot learn smartcard's secret key
- Secure Outsourcing of Scientific Computations
  - Outsourcing scientific computations (matrix multiplication, convolution, etc)
  - No need to design special algorithms for server
  - Pre-processing of data is the key to the secure outsourcing

General Framework



- Pre-processing and post-processing should be as light as possible
- Computation cost for server should be similar to cost of solving problem locally

Outsourcing of Sequence Comparisons

- Application
  - A biological scientist wants to compare two long DNA sequences
  - A smartcard wants to compare two files
- We focus on string edit distance with O(mn) cost
- We design an outsourcing protocol
  - A client outsources sequence comparisons to two servers
  - Servers learns nothings about the original sequences and result
  - Computation cost for client is linear
  - Computation cost for servers is O(mn)

Secure Outsourcing - Issues

- No general solutions for every outsourcing problem
- What is the computation task for the server
  - Same as the algorithm for local computation
  - Specially designed algorithm
- How to prevent server from cheating
  - Server does less work
  - Server tries to figure out client's real data
- In multi-server model, how to prevent collusion

Outsourcing of Image Processing

- Application
  - Weak surveillance camera captures images
  - Protect privacy of images
- We are investigating following problems
  - Secure outsourcing of edge detection problem
  - Secure outsourcing of image matching
- Research on this problem is still ongoing

PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center