Secure and Private Distributed Coded Computation for Learning and Storage Applications

Joerg Kliewer

New Jersey Institute of Technology, Department of Electrical and Computer Engineering

jkliewer@njit.edu, web.njit.edu/~jkliewer

The objective of this project is to investigate information-theoretically secure networked coded computation approaches for machine learning and distributed storage applications.

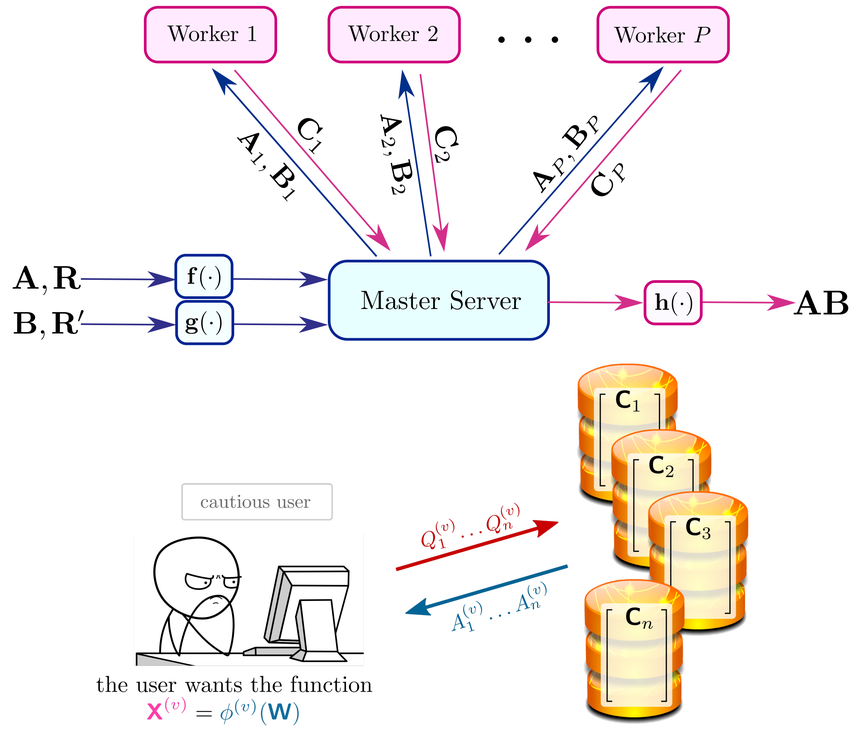
Key topics studied:

Distributed secure matrix computation

- Large scale matrix multiplications are central to machine learning applications as in recommender systems
- Computations are outsourced to the cloud with untrusted commercial off-the-shelf servers prone to failures and straggling
- How to minimize upload and download rate to the cloud?

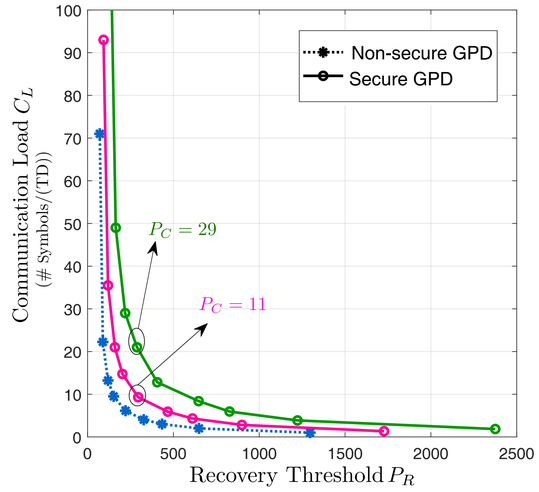
Distributed private function computation

- Computation over untrusted networked databases while minimizing download rate, function must be private to the databases
- Example applications: Computing statistics over medical records, large auctions, tracking satellite anomalities



Key innovations/discoveries:

- Matrix computation: Tradeoff between recovery threshold and communication load
- Compared to downloading a single file, linear private function computation is *free* and achieves an *optimal* download rate
- Reed-Solomon code based homomorphic polynomial computation scheme for coded databases



Broader Impact

Society:

- Advancing information technology and its benefits to society through newly established theory and practice of secure function computation

Education and outreach:

- Impact on underrepresented communities (two female Ph.D. student have been hired on the project).

Potential impact:

- On fields where secure and private function computation is required:
  - Large tensor operations in machine learning
  - Computation of a utility function under a privacy constraint (trade-off between privacy and utility)