Yan Huang

End Data Breaches with Extreme-Scale Secure Multi-party Computation

COLLABORATORS
Ruiyu Zhu
Darion Cassel
Changchang Ding

INDIANA UNIVERSITY
SCHOOL OF INFORMATICS, COMPUTING, AND ENGINEERING
Data is Super Useful
Overwhelming Data, Devastating Breaches

Can we do something to overturn this trend?
Secret Sharing
Secret Sharing

Why not simply attack \textit{at the point of recombining}?
Secure Multiparty Computation

Secret-sharing invented by Shamir and Blakley in 1979, independently.

Secure two-party computation proposed by Yao in 1986.

Many MPC prototypes were built, mostly for two-party, semi-honest setting.

1970s 2000s 2010s 2018

Fancy! But how scalable is your trick?

Without ever recovering the data throughout the process.

AES(k, m) --- 6800 AND gates
Extreme-Scale MPC Protocols

Use cases: secure data mining, secure human genomics, secure & smart power-grids

Our recent work scales MPC techniques to the extremes:

✓ We can securely execute computations of arbitrary size
✓ It allows dividing data into an arbitrary number of shares
✓ Only use off-the-shelf inexpensive hardware
  • Suitable to run on smartphones, watches, smart-meters, drones
Combine MPC with Blockchains

- Revolutionize blockchain mining for useful work.
- Publicize one’s own sensitive data for profit.
- More efficient MPC against rational adversaries.
THANK YOU

Yan Huang
yh33@iu.edu
http://homes.soic.indiana.edu/yh33/