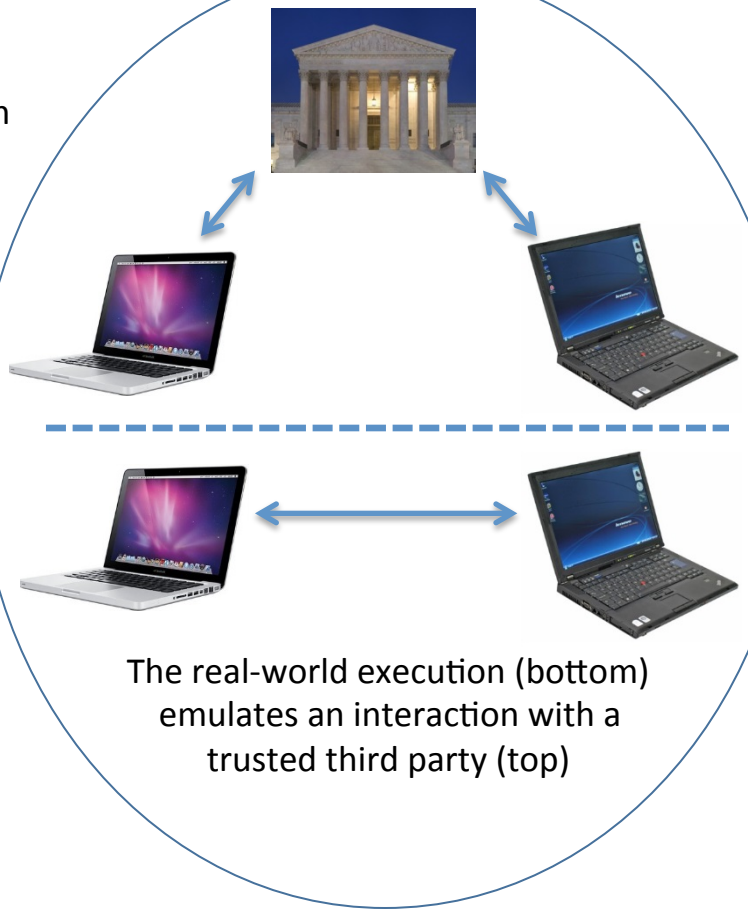
Practical Secure Two-Party Computation: Techniques, Tools, and Applications

EMP
Efficient Multi-Party computation toolkit

Challenge:

- Enable efficient computation on data held by two parties, without revealing anything about one party's data to the other



The real-world execution (bottom) emulates an interaction with a trusted third party (top)

Scientific Impact:

- Security against *malicious* adversaries can be achieved with significantly better efficiency than previously known
- This brings secure two-party computation even closer to practice

Solution:

- The *theory* of secure computation has been studied for decades
- We are developing new techniques to vastly improve *efficiency* while retaining provable security

Broader Impact:

- Potential applications in finance, data mining, DNA testing, and more
- Interest from DoD, NIST, OFR
- Several startups exploring commercialization

CNS-1111599, University of Maryland in collaboration with UVA and Indiana University. jkatz@cs.umd.edu