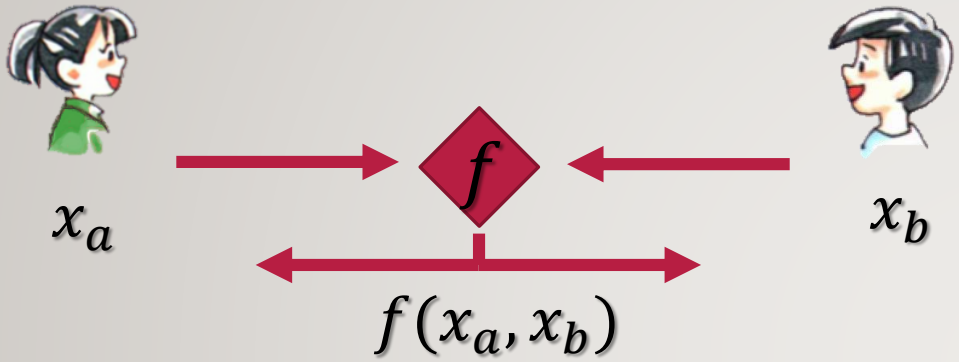
Faster Malicious 2-party Secure Computation with Online/Offline Dual Execution

Peter Rindal
Mike Rosulek

Oregon State University OSU

Applications and techniques



Techniques

- Yao's garbled circuits
- Secure sharing based

Applications

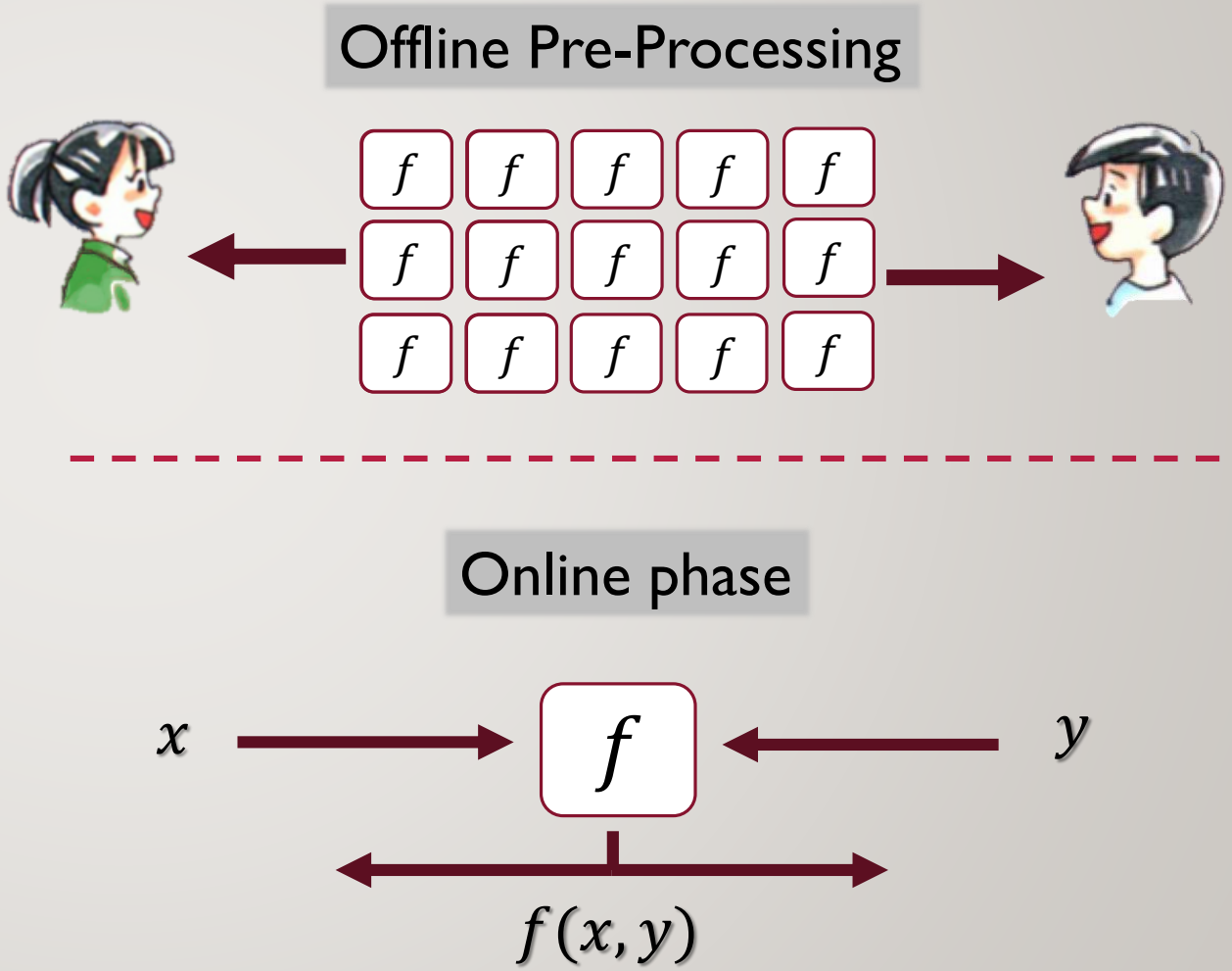
- Private database querying

- Joint Machine learning

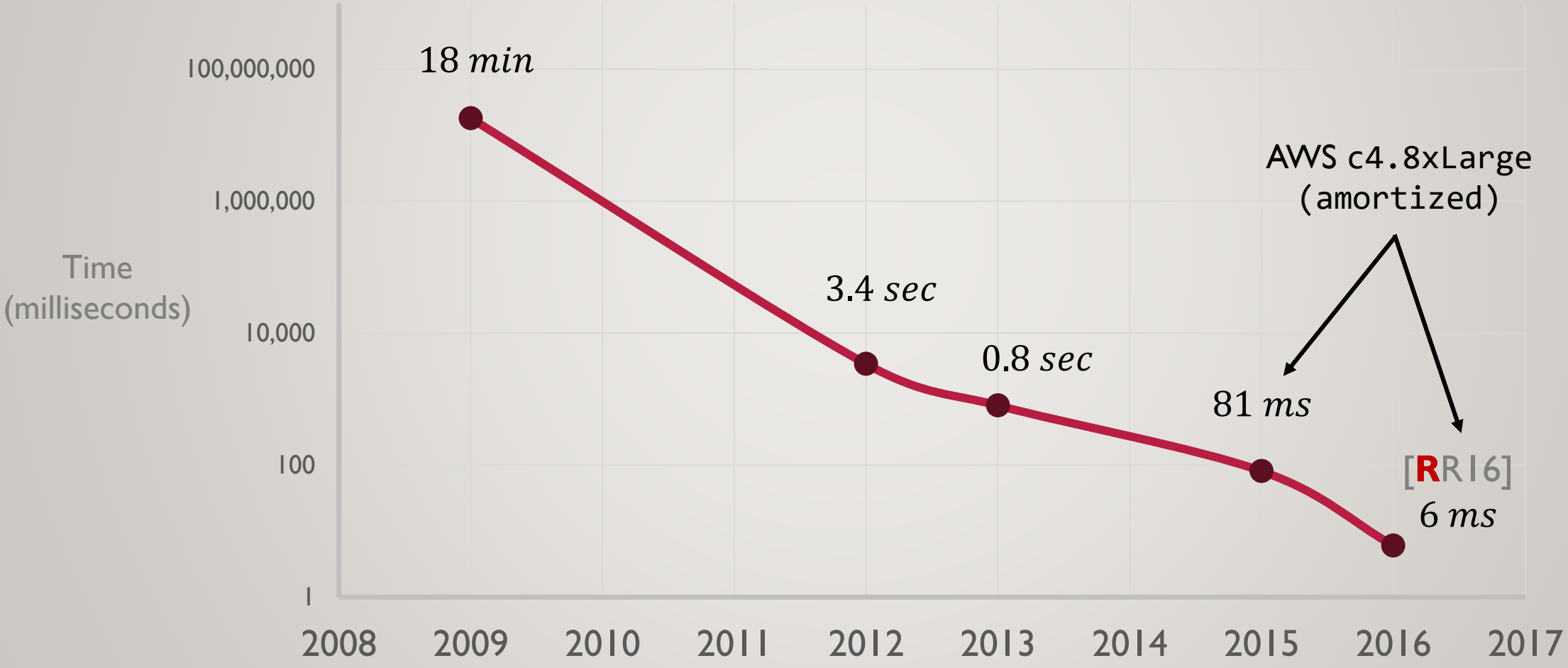
- Secure auctions

Faster Malicious 2PC with Online/Offline Dual Execution

- Want to execute f many times
  - Perform pre-processing
  - Evaluate one f in the online phase
- Amortize garbled circuit overhead
- Performance
  - Online + Offline AES in $6\ ms$



Total Protocol Times for AES



Faster Malicious 2-party Secure Computation with Online/Offline Dual Execution

Applied Cryptography track @ 4:30

Peter Rindal
Mike Rosulek

Oregon State UNIVERSITY OSU