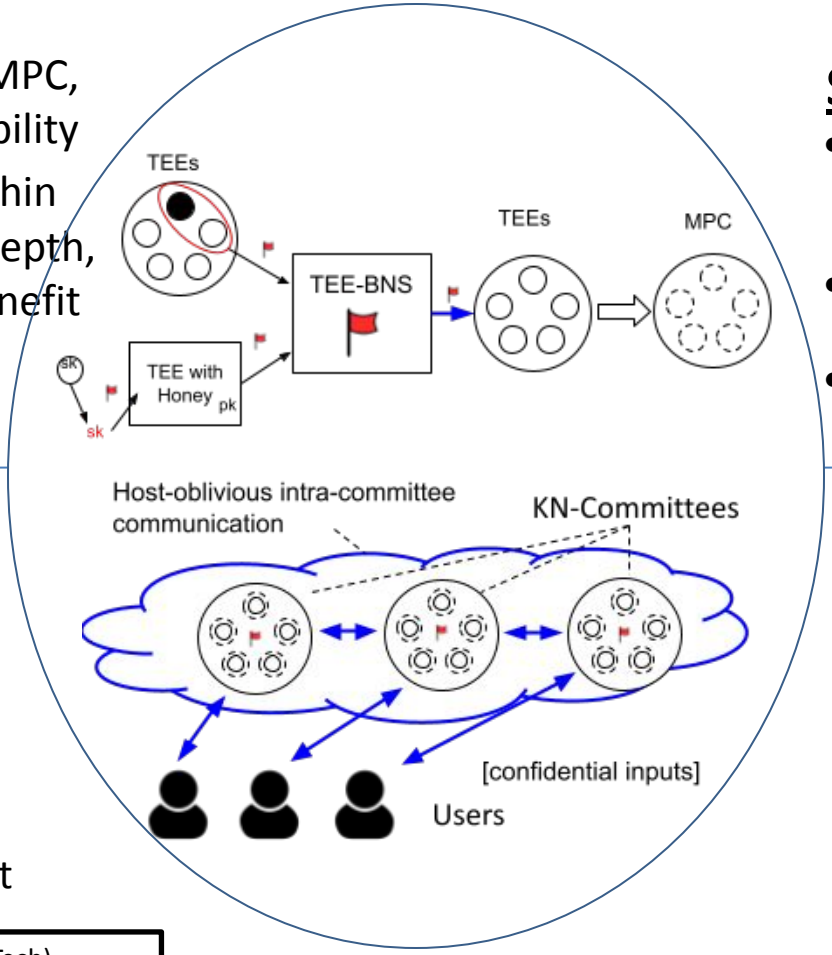
SATC: CORE: Medium: Collaborative: Hybridizing Trusted Execution Environments and Secure Multiparty Computation

Challenge:

- TEEs can be faster than MPC, but must mitigate vulnerability
- Naively running MPC within TEEs provides defense in depth, but spoils performance benefit relative to MPC



Solution:

- Use MPC to harden TEE applications
  - TEE with MPC as failover
  - TEE as honey objects
- Use TEEs to accelerate MPC preprocessing
- Adaptive security through oblivious TEE task assignment

Scientific Impact:

- Redundant execution on TEEs to detect compromise
- New mobile adversary model with TEEs
- Horizontal scaling with TEE committees

Broader Impact and Broader Participation:

- Motivating application: an Identity System for bridging real world identities and blockchain applications
- Software artifact: Auditee library for reproducible builds, oblivious data

Andrew Miller (UIUC), Ari Juels (Cornell Tech)

Project #s 2112726 (UIUC) 2112751(Cornell Tech)