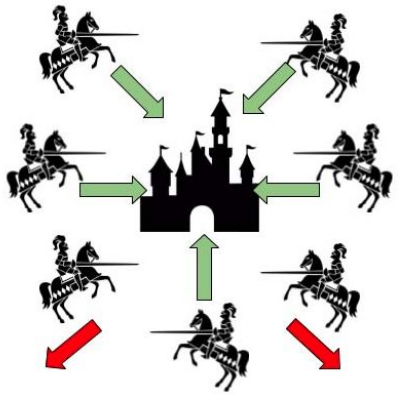
Efficient and Secure Distributed Consensus

Charalampos Papamanthou

Goals

- Distributed consensus useful in Blockchains, MPC, etc.
- Flavours: Byzantine Broadcast, State machine replication, etc.
- Improve efficiency in dishonest majority:
  - Communication and round complexity
- Improve security to handle network adversaries:
  - Strongly adaptive: State actors/autonomous systems
  - Mobile sluggish faults: Synchronous and part. synchronous



Solution

- Communication of Byzantine (Parallel) Broadcast (P)BC:
  - **Linear factor** improvement BC & PBC **without** trust assum.
  - **Linear factor** improvement PBC with trust assumptions
    - Efficient gossiping dissemination
- Improving security (block network adversaries):
  - BC compiler from weakly to **strongly** adaptive
  - **First** mobile sluggish protocol in permissionless setting!
    - Uses time-lock puzzles
- First **expected constant round** BC (in strongly adaptive)

Broader Impact

- Helping users improve their security and privacy
- Placement of graduate students to positions in industry and academia

Scientific Impact

- Solutions to long standing open problems in (P)BC
- Shows that there are no fundamental barriers

Award # 1652259:
CAREER: Towards Practical Systems for Trustworthy Cloud Computing