Proof of Work Without All the Work

PIs: Jared Saia and Maxwell Young (#1816250 and #1816076)

Highlight Slide for SaTC Principal Investigator's Meeting 2019

Challenge:

Proof of work (***PoW***) is popular tool for securing open systems from ***Sybil attack***

But high cost for solving puzzles perpetually, regardless of severity of attack

Prior PoW-based defenses do not scale

Scientific Impact:

Secure and scalable systems where good IDs have computational cost that is a slow-growing function of attacker's cost

Solution:

Algorithm that guarantees with high probability under dynamic joins/departures:

- Majority of IDs are good
- Small committee is known to all good IDs for scalable agreement
- Total cost to good IDs is $O(J + \sqrt{T(J+1)})$ where ***T*** is cost of attacker and ***J*** is join rate of good IDs

Broader Impact

Extensions to several network scenarios for broad use: Committee-less version, overlay networks, application to DDoS attacks

Annual workshops between theorists and practitioners in the area