Adaptively Secure Multi-Party Computation with Dishonest Majority

Sanjam Garg Amit Sahai

UCLA

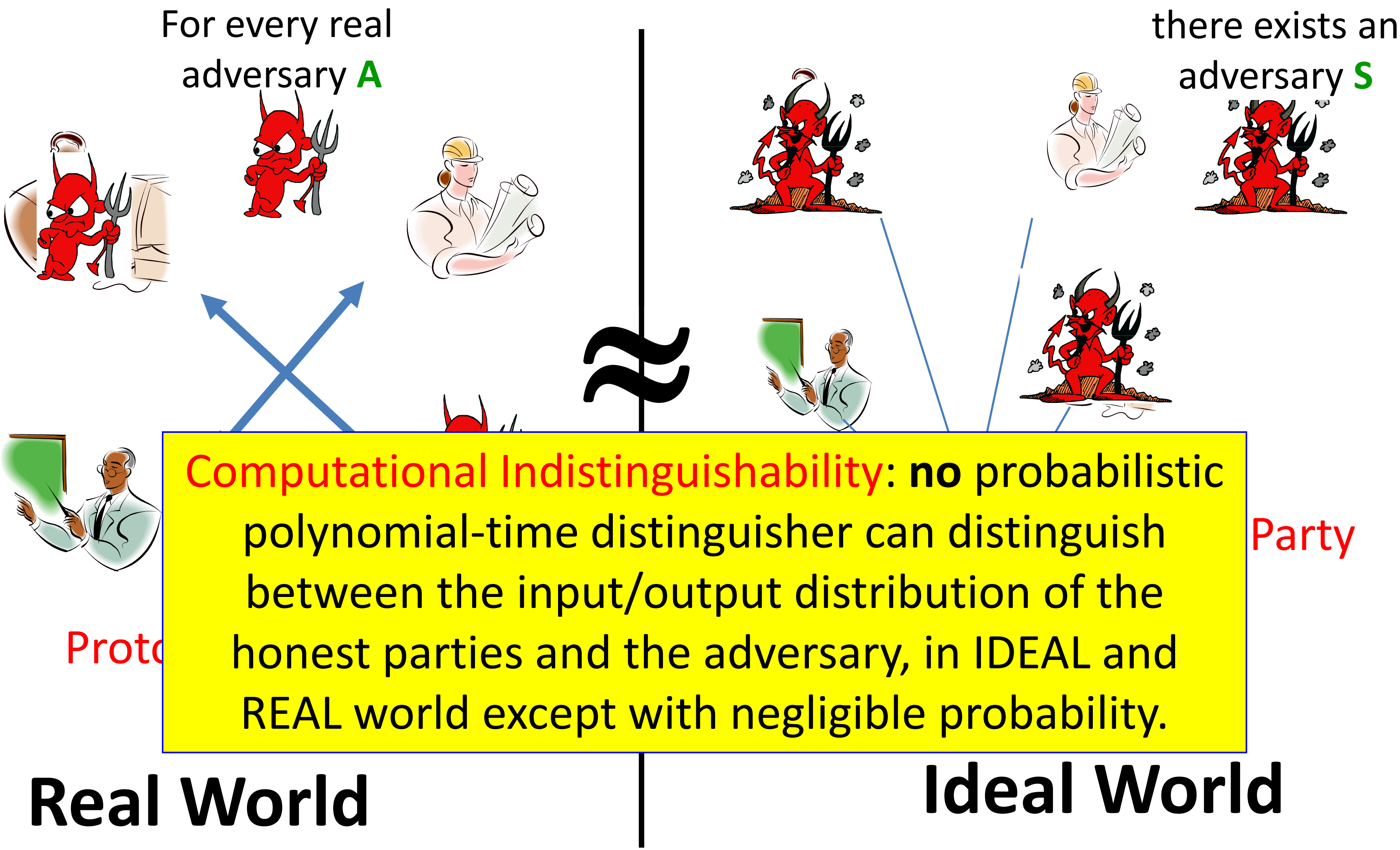
Secure Multiparty Computation

- A set of mutually distrustful parties (n) wish to compute a joint function of their private inputs [Yao86, GMW87]

- Adaptive Adversaries: Security desired in face of arbitrary malicious behavior by some of the participants that adversary chooses on the fly [CFGN96]

- Very fundamental notion in cryptography

Multiparty Computation



Computational Indistinguishability: **no** probabilistic polynomial-time distinguisher can distinguish between the input/output distribution of the honest parties and the adversary, in IDEAL and REAL world except with negligible probability.

Motivating Example: a secret sharing protocol [CFGN96]

- Consider a setting with n parties and a dealer with a secret sk
- Dealer secret shares sk among random $\sqrt{n}$ parties (and publishes the set of parties that get the shares)
- Consider an adversary that can corrupt $t = O(n)$ out of n parties
- Non-Adaptive (or Static) adversary succeeds in obtaining secret with the negligible probability
- While Adaptive adversary always succeeds

Previous Results

- Adaptively secure MPC protocol in the standalone setting assuming honest majority. [CFGN96]
- Doing better that honest majority
  - ZK and OT [Bea96a,Bea96b]
  - two-party computation [Bea98, KO04]
  - adaptively secure MPC protocol without honest majority but using a common random string [CLOS02]

Can we do adaptively secure MPC without honest majority and without assuming a trusted setup?

A very simple approach

- We know
  - adaptively MPC when given access to an ideal commitment [e.g. CLOS02, CDMW09, GWZ09]
  - adaptively secure protocols for securely realizing the commitment functionality (e.g. [Bea98, PW09])
  - Composition theorem of Canetti [Can00]
- Surprisingly direct application of these results does not yield adaptive MPC.
- This subtle issue was overlooked in the literature as it was thought as obvious.
- Let's see why!

Adaptively Secure Composition: More than Meets the Eye

- 2-party adaptively secure protocol does not guarantee security in the setting of n-parties, even if only two of the parties are ever talking to each other (quiet parties also have secret state)
- Consider an adaptive 2PC protocol with a black-box simulation
- Relies on rewinding
- In the n-party case adversary can also corrupt parties that do not communicate
- This was never handled in the 2-party case…

Our Results

constant round

if corruption of up to n-1 parties is allowed (in non-erasure model)

Or if erasures are allowed

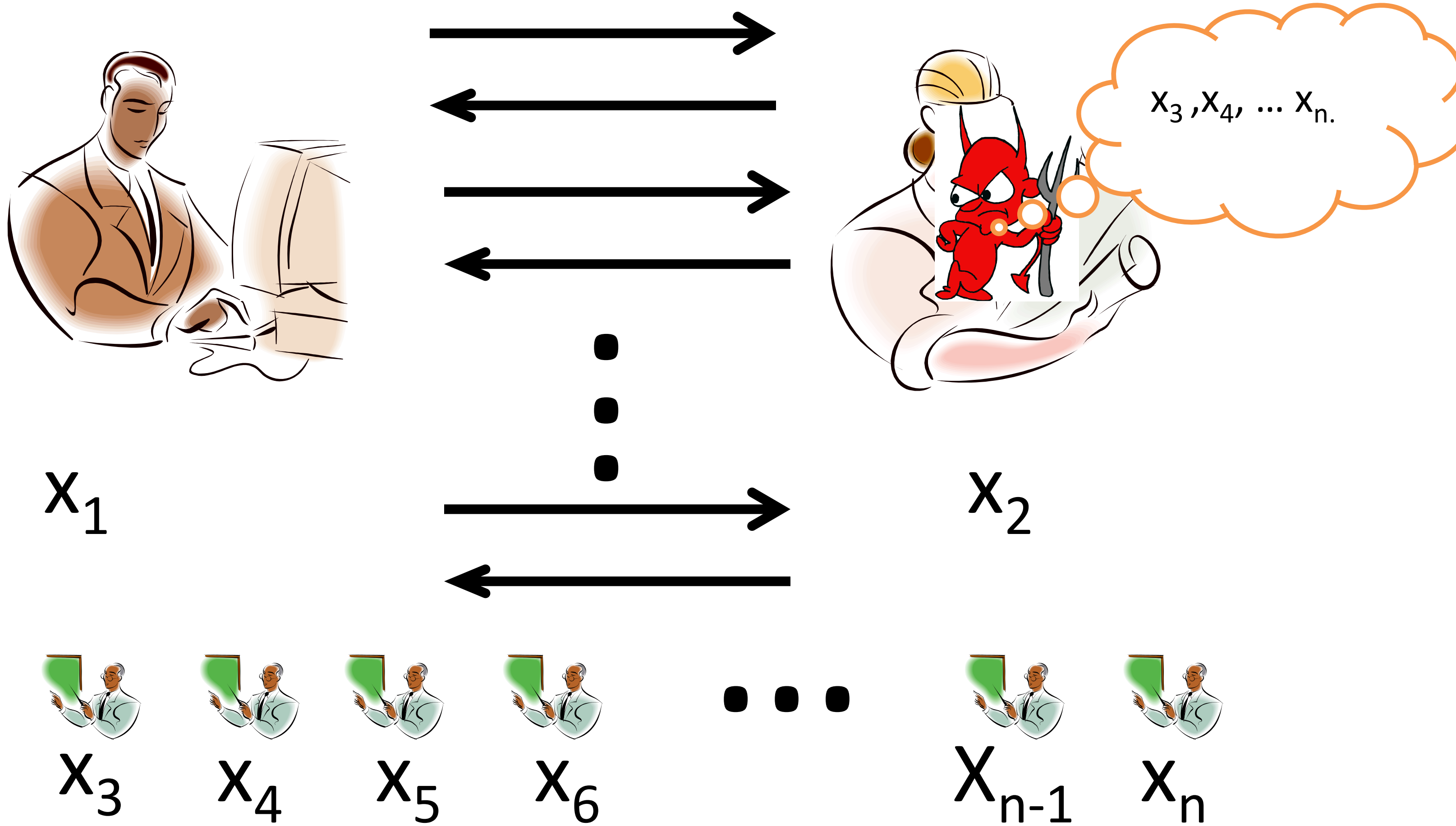
Linear in depth of circuit otherwise

Does not old in the setting of Super-polynomial simulation

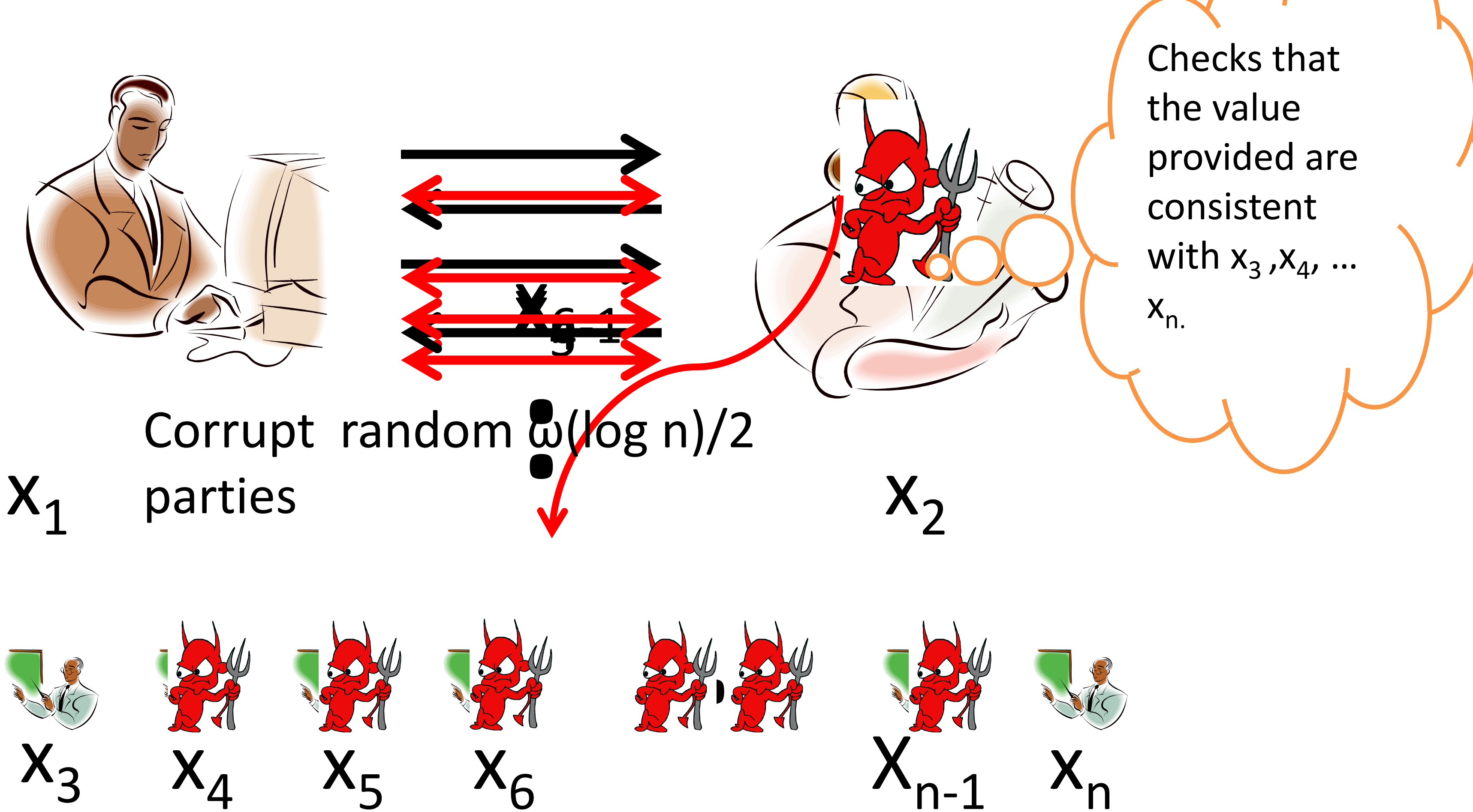
– As good as semi-honest setting

Impossibility Result – Building the rewinding intuition

Consider $o(n/\log n)$ round protocol between 2-parties

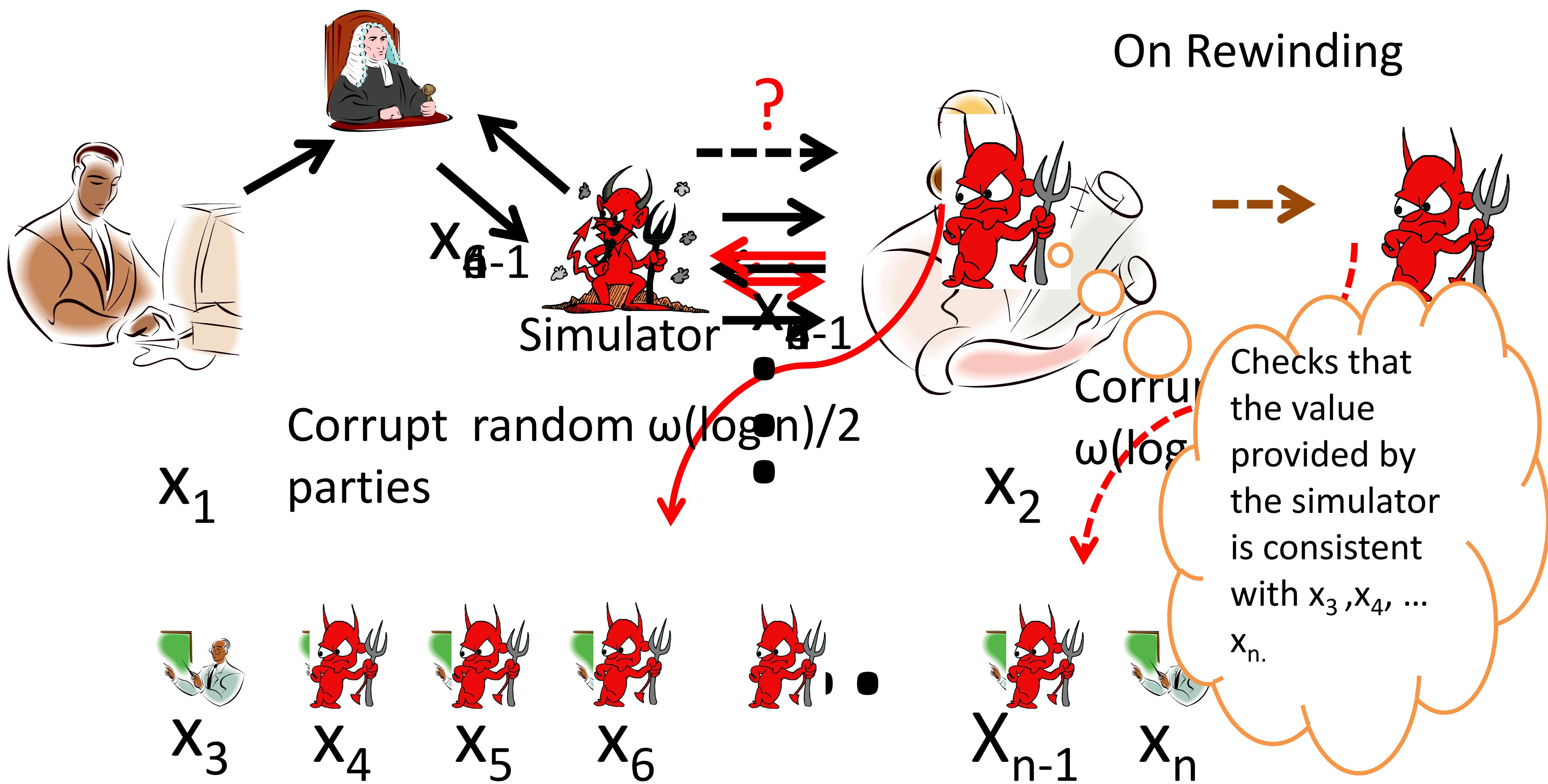


Real World Execution



The protocol has o(n/log n) rounds and so a maximum of n/2 parties are corrupted in the main execution

Rewinding by simulator



At least one party different from the n/2 parties corrupted in the main execution is corrupted

Implications of the above problem

- The simulator can not rewind in any round
  - This allows us to conclude that using black box simulation round efficient adaptive MPC is impossible
- Circumvent this with large round complexity
  - There always exists a round where no one is corrupted
  - Other issues of non-malleability
  - But we focus on a constant round protocol using non-black box simulation

Constant round protocol

- We can not rewind the adversary
- Straight line or non-rewinding simulation
  - non-black box simulation technique of Barak
  - Problem is that Barak's protocol is far from being adaptively secure
- How do we get it to work?

Conclusions

- [CFGN96] constructed the first adaptive secure MPC protocol in the setting of honest majority
  - Left open the question in the setting of dishonest majority
- We resolve this question
  - non-black box simulation is essential for round efficient solutions

Thank You!